Reuben D. Nathan, Esq. (SBN 208436)
NATHAN & ASSOCIATES, APC
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff SALEHA ABDULLAH

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SALEHA ABDULLAH, on behalf of herself and all similarly situated persons, Plaintiff, v. DISNEY DTC LLC, a Delaware limited liability company, Defendant.	Case No. **COMPLAINT** **CLASS ACTION**

I. NATURE OF THE ACTION

1. Defendant DISNEY DTC LLC, a Delaware limited liability company (referred to herein as "Defendant" or "DISNEY") owns and operates a website, www.espn.com (the "Website").

2. This is a class action lawsuit brought by Plaintiff SALEHA ABDULLAH ("Plaintiff") on behalf of herself and on behalf of all California residents who have accessed the Website ("Class Members").

3. Plaintiff files this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Defendant. Plaintiff brings this action based upon personal knowledge of the facts pertaining to her, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

4. A pixel tracker, also known as a web beacon, is a tracking mechanism embedded in a website that monitors user interactions. It typically appears as a small, transparent 1x1 image or a lightweight JavaScript snippet that activates when a webpage is loaded or a user performs a tracked action.

5. When triggered, the pixel transmits data from the user's browser to a third-party server. This data typically includes page views, session duration, referrer URLs, IP address, browser and device details, and other interaction metadata.

6. When users visit the Website, Defendant causes tracking technologies to be installed, executed, embedded, or injected in visitors' browsers. These include, but are not limited to, the following:

- Google Ads / DoubleClick / Tag Manager Tracker
- Rubicon / Magnite Tracker
- Comscore Tracker

7. The third parties who operate the above-listed trackers use pieces of User Information (defined below) collected via the Website as described herein for their own independent purposes tied to broader advertising ecosystems, profiling, and data

monetization strategies that go beyond Defendant's direct needs for their own financial gain. The above-listed trackers are referred to herein collectively as the "Trackers."

8. The trackers present on Defendant's Website include technologies operated by major third-party advertising, bid-exchange, and audience-measurement companies, specifically Google LLC (Google Ads, DoubleClick, and Google Tag Manager), Magnite, Inc. (formerly Rubicon Project), and Comscore, Inc. (ScorecardResearch). Defendant embeds and enables these technologies on the Website, causing Plaintiff's browser to transmit signaling, routing, addressing, device, and behavioral information directly to these Third Parties' servers. These transmissions allow Google's advertising ecosystem to perform targeted advertising, retargeting, and real-time bidding; enable Magnite's exchange infrastructure to ingest identifiers and bid-stream metadata for auction and profiling purposes; and permit Comscore to collect audience-measurement, behavioral, and device-level information for analytics, segmentation, and downstream data products within the ad-tech ecosystem. Magnite, Inc. and Comscore, Inc. are both registered data brokers in California.

9. Plaintiff is informed and believes, and thereon alleges, that Defendant has additionally implemented third-party audience-measurement and behavioral-tracking technologies operated by Nielsen (including Nielsen's digital measurement and tagging infrastructure). These technologies function as third-party listeners that activate upon user interaction with the Website and receive users' signaling, routing, addressing, device, and behavioral information. Plaintiff is informed and believes that Nielsen uses this data to generate audience-measurement metrics, construct behavioral segments, and associate users with pseudonymous identifiers within its cross-site analytics and measurement ecosystem, operating in the same manner as the other Trackers alleged herein. The Nielsen Company is a registered California data broker.

10. Through the Trackers, the Third Parties collect detailed user information including IP addresses, browser and device type, screen resolution, operating system, pages visited, session duration, scroll depth, mouse movements, click behavior, referring

URLs, unique identifiers (such as cookies and ad IDs), and geolocation based on IP. This information is used for behavioral profiling, ad targeting, cross-device tracking, and participation in real-time advertising auctions (collectively, "User Information").

11. Because the Trackers capture and transmit users' IP addresses, full page URLs, referrer headers, device identifiers, and other non-content metadata, they function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code § 638.50. These tools silently collect routing and addressing information for commercial use without user interaction, as defined in Greenley v. Kochava, Inc., 2023 WL 4833466 (S.D. Cal. July 27, 2023).

12. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices and did not expect their behavioral data to be disclosed or monetized in this way. By installing and using the Trackers without prior consent and without a court order, Defendant violated CIPA section 638.51.

13. By installing and activating the Trackers without obtaining user consent or a valid court order, Defendant violated California Penal Code § 638.51, which prohibits the use of pen registers and trap and trace devices.

14. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents.

15. Generalized references herein to users, visitors and consumers expressly include Plaintiff and the Class Members.

II. PARTIES

16. Plaintiff SALEHA ABDULLAH is a California citizen residing in Contra Costa County and has an intent to remain there. Plaintiff was in California when she visited the Website, which occurred during the class period prior to the filing of the complaint in this matter. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

/ / /

17. DISNEY DTC LLC is a Delaware limited liability company that owns, operates, and/or controls the Website which is an online platform that offers online services and digital content to consumers.

18. DISNEY owns and operates the Website (www.espn.com), which serves as the primary consumer-facing digital platform for ESPN, a leading global sports media and entertainment brand, in the United States. Through the Website, DISNEY provides millions of users with live and archived sports content, breaking news, scores, standings, statistics, fantasy-sports tools, streaming integrations, and advertising-supported digital media experiences.

19. While ESPN content is distributed across multiple channels, including mobile applications and connected television interfaces, the Website independently provides a full suite of digital publishing, advertising, and audience-engagement services. The Website is responsible for delivering customized sports coverage, serving advertising inventory, and integrating with ESPN's subscription and streaming infrastructure, including ESPN+. In operating this digital media platform, DISNEY collects and processes substantial volumes of user data for purposes that include content personalization, ad-delivery optimization, audience measurement, behavioral analytics, and digital advertising.

20. The Website functions as ESPN's primary digital storefront and media distribution hub. It allows users to access real-time sports scores, watch highlights, read articles, log into subscriber accounts, manage fantasy sports teams, and stream programming through linked ESPN services. In addition to these content-distribution functions, the Website also operates as a data-collection and behavioral-tracking platform controlled by DISNEY through which user interactions are monitored, profiled, and monetized within ESPN's advertising ecosystem.

21. Through the deployment of third-party tracking technologies, including advertising pixels, event-tracking scripts, device-fingerprinting tools, audience-measurement tags, and programmatic advertising integrations, DISNEY collects

granular data about user interactions with the Website. These data practices form a core component of ESPN's performance marketing, ad targeting, cross-platform analytics, and audience-monetization strategies, enabling DISNEY and its advertising partners to deliver targeted advertising, measure engagement, and construct user-level behavioral profiles.

III. JURISTICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the total matter in controversy exceeds $5,000,000 and there are over 100 members of the proposed class. Further, at least one member of the proposed class is a citizen of a State within the United States and at least one defendant is the citizen or subject of a foreign state.

23. DISNEY does business at 500 South Buena Vista Street, Burbank, California 91521 according to its Website Terms of Use, which is a direct admission of continuous business operations at a California address.

24. Venue is proper in the Northern District of California pursuant to 28 U.S.C. § 1391 because Defendant (1) is authorized to conduct business in this District and has intentionally availed itself of the laws and markets within this District; (2) does substantial business within this District; (3) Plaintiff resides in this District; and (4) the injury to Plaintiff occurred within this District

IV. GENERAL ALLEGATIONS

A. The California Invasion of Privacy Act (CIPA)

25. Enacted in 1967, the California Invasion of Privacy Act is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging surveillance technologies, stating that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat

to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

26. CIPA specifically prohibits the installation or use of "pen registers" and "trap and trace devices" without consent or a court order. Cal. Penal Code § 638.51(a).

27. A "pen register" is defined as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," excluding the contents of the communication. Cal. Penal Code § 638.50(b).

28. Conversely, a "trap and trace device" is a device or process that captures "incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication," again excluding the contents. Cal. Penal Code § 638.50(b).

29. In practical terms, a pen register is a device or process that records outgoing dialing information, while a trap and trace device is a device or process that records incoming dialing information.

30. Historically, law enforcement has utilized these devices to monitor telephone calls, with pen registers recording outgoing phone numbers dialed from a specific line and trap and trace devices recording the phone numbers of incoming calls to that line.

31. Although originally focused on landline telephone calls, CIPA's scope has expanded to encompass various forms of communication, including cell phones and online interactions. For instance, if a user sends an email, a pen register could record the sender's email address, the recipient's email address, and the subject line, essentially capturing the user's outgoing information.

32. Similarly, if the user receives an email, a trap and trace device could record the sender's email address, the recipient's email address, and the subject line, capturing the incoming information.

33. Despite predating the Internet, CIPA has been interpreted by the California Supreme Court to apply to new technologies where such application does not conflict with the statutory scheme. In re Google Inc., 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); see also, e.g., Shah v. Fandom, Inc, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); Mirmalek v. Los Angeles Times Communications LLC, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); Moody v. C2 Educ. Sys. Inc. 742F. Supp. 3d 1072, 1076 (C.D. Cal. 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); Greenley, supra, at 1050 (referencing CIPA's "expansive language" when finding software was a "pen register"); Javier v. Assurance IQ, LLC, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications. This interpretation aligns with the principle that CIPA should be construed to provide the greatest privacy protection when faced with multiple possible interpretations. Matera v. Google Inc., 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

34. The conduct alleged herein constitutes a violation of a legally protected privacy interest that is both concrete and particularized. Invasions of privacy have long been actionable under common law. Patel v. Facebook, 932 F.3d 1264, 1272 (9th Cir. 2019); Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017).

35. Both the legislative history and statutory language indicate that the California Legislature intended CIPA to protect core privacy rights. Courts have found that violations of CIPA give rise to concrete injuries sufficient to confer standing under Article III. See Campbell v. Facebook, Inc., 2020 WL 1023350; In re Facebook Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020).

/ / /

36. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation. Cal. Penal Code § 637.2(a)(1).

B. The Trackers Are "Pen Registers" and/or "Trap and Trace Devices"

37. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request or "GET" request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP response containing the necessary resources, including HTML, cascading style sheets (CSS), JavaScript files, and image assets, used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. The server's instructions include how to properly display the Website, e.g., what images to load, what text should appear, or what music should play.

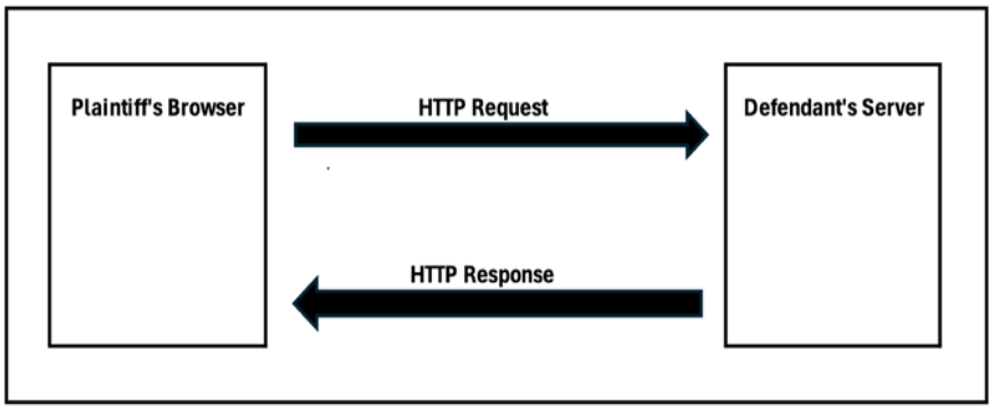
38. In addition, the server's instructions included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. The instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's IP address and User Information to the Third Parties. These Third Parties, through their Trackers, also set cookies on Website users' browsers, which sends a unique identifier to these Third Parties that allows them to track users on the Website over multiple visits and across the Internet.

39. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests.

/ / /

/ / /

Figure 1:



40. The server's response included third-party tracking scripts that were executed by the Plaintiff's and Class Members' web browsers. These scripts, once executed, initiate client-side functions that capture routing and behavioral metadata and transmit this data, typically via HTTPS requests, to the servers of third-party tracking vendors. These actions occur without visible indicators or user awareness. The transmitted data, the User Information, is used to profile users and facilitate targeted advertising.

41. The Trackers operate by initiating HTTP or HTTPS requests using either the GET or POST method from the user's browser to external servers controlled by the Third Parties. These requests are triggered by user interactions with the Website and are used to transmit behavioral data and Device Metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

42. Plaintiff and Class Members did not provide their prior consent to Defendant to install the Trackers on their browsers or use the Trackers. Nor did Defendant obtain a court order before installing or using the Trackers.

43. An IP address is a numerical identifier assigned to each device or network connected to the Internet, used to facilitate communication between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.*, (9th Cir. 2019) 938 F.3d 985, 991 n.4. The most common format, known as IPv4, consists of four numbers separated by periods (*e.g.*,

191.145.132.123). IPv4 is the traditional format of IP addresses and, because it has a finite amount of combinations, it is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[1]

44. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices. IP addresses can be used via external geolocation services to infer a user's general location, including state, city, approximate latitude and longitude, and in some cases, ZIP code.

45. Public IP addresses are globally unique identifiers assigned by Internet Service Providers ("ISPs") that allow devices to communicate directly over the Internet. They are globally accessible, meaning they can be reached from anywhere on the Internet, but are not inherently exposed unless data is being transmitted. Public IP addresses are essential for devices requiring direct Internet access.

46. Public IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io, use databases that map IP addresses to geographic areas, often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP. This geolocation capability is leveraged by online advertising and user identification services.

47. In contrast, private IP addresses are used within internal networks and are not routable on the public Internet. The Internet Assigned Numbers Authority ("IANA") reserves specific ranges of numbers to be exclusively used for private IP addresses (*e.g.*,

[1] *See*, *e.g.*, *What is the Internet Protocol*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/; Stefano Gridelli, *What is an RFC1918 Address?*, NETBEEZ (Jan. 22, 2020), https://netbeez.net/blog/rfc1918/.

172.16.0.0 through 172.31.255.255). They are isolated from the global Internet and can be reused across different networks without conflict. For example, a home network in New York and an office network in Tokyo can both use the same private IP address (*e.g.*, 192.168.1.1) for their routers without conflict.

48. The distinction between a public and private IP address is fundamental to the architecture of modern networks. Public IP addresses facilitate global communication, while private IP addresses conserve the finite amount of combinations to make an IP address through local network communication. And crucially, a private IP address does not divulge a user's geolocation, whereas a public IP address does and is thus extensively used in advertising.

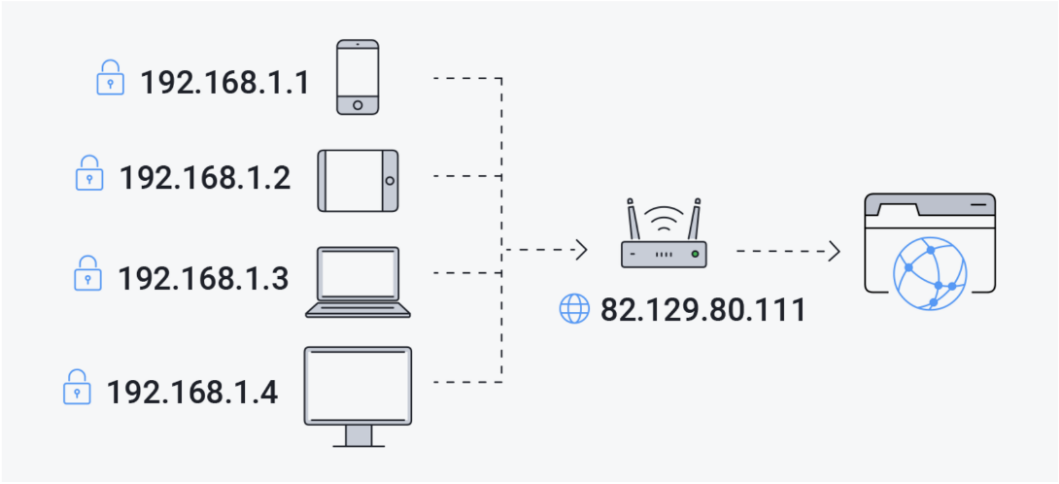
49. An analogy is useful. A public IP address is like the number for a landline telephone for a household. A private IP address is like each handset that is connected to that landline number (*e.g.*, "Handset #1," "Handset #2"). A lot can be gleaned from knowing the phone number that is making the call, while knowing Handset #1 versus Handset #2 is making a call provides additional information.

50. The same is true of IP addresses. The public IP address divulges the approximate location of the user that is connecting to the Internet and the router directing those communications (presumably the user's house or workplace), and it is the means through which the user actually communicates with the website and the Internet at large. The private IP address then distinguishes between the devices accessing the same public IP address.[2]

/ / /

[2] While the Trackers do not collect private IP addresses, as discussed below, the Trackers also collect Device Metadata, which distinguishes between devices accessing the same public IP address. So, by installing the Trackers on Website users' browsers, Defendant allows third parties to collect information that is analogous to a telephone number (the public IP address) and the specific handset that is making the call (the "Device Metadata").

Figure 2:



Each device on a network has a private IP address, and the router has a public IP address to communicate with the rest of the internet.

51. Thus, the differences between public and private IP addresses are as follows:[3]

Figure 3:

Category	Private IP address	Public IP address
Scope	The private IP address only has a local scope in your own network.	The public IP address's scope is global.
Communication	It is used so devices within a network can communicate with each other.	It allows access to the internet and is used for communication outside of your own network.
Uniqueness	It's an address from a smaller range that's used by other devices in other local networks.	It's a unique address that's not used by other devices on the internet.
Provider	The router assigns a private IP address to a specific device on the local network.	The internet service provider assigns the public IP address.
Range	Private IP address ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Any IP address that isn't within a private IP address range.

[3] WHAT'S THE DIFFERENCE BETWEEN A PUBLIC AND PRIVATE IP ADDRESS?, AVIRA (Jan. 31, 2024), https://www.avira.com/en/blog/public-vs-private-ip-address.

52. A public IP address is therefore "routing, addressing, or signaling information." A public IP address functions as "routing, addressing, or signaling information" by facilitating internet communication. It provides essential information that can help determine the general geographic coordinates of a user accessing a website through geolocation databases. Additionally, a public IP address is involved in routing communications from the user's router to the intended destination, ensuring that emails, websites, streaming content, and other data reach the user correctly.

53. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet. It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

54. A public IP address is "addressing" information because it determines the general geographic coordinates of the user who is accessing a website.

55. A public IP address is "routing" or "signaling" information because it is sending or directing the user's communication from the router in their home or work to the website they are communicating with, and ensuring that "emails, websites, streaming content, and other data reaches you correctly."[4]

56. Through a public IP address, a device's state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user's public IP address and therefore geographical location "provide[s] a level of specificity previously unfound in marketing."[5]

/ / /

/ / /

[4] Anthony Freda, *Private IP vs Public IP: What's the Difference?*, AVG (June 4, 2021), https://www.avg.com/en/signal/public-vs-private-ip-address.

[5] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

57. A public IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code" [6] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests." [7] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service" [8] because "[c]ompanies can use an IP address … to personally identify individuals." [9]

58. In fact, a public IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs." [10] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event. [11]

59. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP)

---

[6] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.

[7] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://tinyurl.com/c2ne77ua.

[8] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[9] Trey Titone, *The Future Of IP Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[10] *See, e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.

[11] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location." [12]

60. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data." [13]

61. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's public IP address because it "can be more cost-effective than other forms of advertising." [14] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience." [15]

62. In addition, "IP address targeting can help businesses to improve their overall marketing strategy." [16] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts." [17]

63. The collection of IP addresses here is particularly invasive here: As a report from NATO found:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website]

---

[12] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.

[13] *Id.*

[14] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[15] *Id.*

[16] *Id.*

[17] *Id.*

> while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behavior across devices and target the user and their devices with ads on different networks. [18]

64. In other words, not only does the collection of IP addresses by the Third Parties cause harm in and of itself, data brokers use IP addresses to identify users, append the IP address to a unique profile containing even more information about the user, attach specific IP addresses to comprehensive user profiles, and track Plaintiff and Class Members across the Internet using their IP addresses, compiling vast reams of other personal information in the process.

65. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual." [19]

/ / /

/ / /

---

[18] HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[19] IS AN IP ADDRESS PERSONAL DATA?, CONVESIO, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also* WHAT IS PERSONAL DATA?, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

66. When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions. [20]

67. Often times, third-party scripts are installed on websites "for advertising purposes." [21]

68. Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time." [22]

69. Defendant has long incorporated the Trackers' code into the code of its Website, including when Plaintiff and Class Members visited the Website. Thus, when Plaintiff visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

70. As described below, when a user visits the Website, the Website's code as programmed by Defendant installs the Trackers onto the user's browser. This allows the Third Parties through their respective Trackers to collect Plaintiff's and Class Members' IP addresses, Device Metadata, and User Information, and pervasively track them across the Internet.

71. Public IP addresses play a significant role in digital marketing by enabling geographic targeting based on a user's approximate location. Through IP geolocation services, advertisers can often determine a user's country, region, city, and in some cases, ZIP code or service area. In contexts where a static IP address is associated with a fixed residence or business, this data can contribute to household-level or business-

---

[20] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[21] *Id.*

[22] *Id.*

level targeting, particularly when combined with other tracking identifiers and third-party enrichment.

72. Defendant and the Third Parties then use the public IP addresses, Device Metadata, User Information, and other information of Website visitors that are collected and set by the Trackers, including those of Plaintiff and Class Members, to deanonymize Plaintiff and Class Members, serve hyper-targeted advertisements, and unjustly enrich themselves through this improperly collected information. Defendant installs Trackers on users' browsers to collect User Information, including IP addresses and full URLs, which constitute outgoing routing and addressing metadata under CIPA. These identifiers serve the same function as telephony dialed numbers and therefore meet the statutory definition of a pen register or trap and trace device.

73. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members' browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members' consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

C. The Use of Trackers or Beacons and Digital Fingerprinting

74. Website users typically expect a degree of anonymity when browsing, particularly when they are not logged into an account. However, upon visiting the Website, Plaintiff's and Class Members' browsers executed third-party tracking scripts embedded by the Defendant. These Trackers operate in the background of the browsing session and collect detailed behavioral and technical information, which is then transmitted to external third-party servers without the users' active awareness.

75. The Trackers also causes additional data points to be sent from Plaintiff's and Class Members' browser to the Third Parties, which are meant to uniquely identify users across sessions and devices. In addition to the public IP address, key elements include the user-agent string (browser, operating system, and device type) and device capabilities such as supported image formats and compression methods. Persistent identifiers like the PUID, GUID, UID, PSVID, and User-Agent ensure users can be

tracked even after clearing standard session data like cookies. Advanced methods like fingerprinting and server-side matching remain unaffected by cookie deletion. Combined, these elements form a detailed, unique fingerprint that allows for cross-site tracking and behavioral profiling.

76. This process, known as digital fingerprinting, involves compiling various data points such as browser version, screen resolution, installed fonts, device type, and language settings to generate a unique identifier for each user. Fingerprinting can be used to recognize repeat visits and correlate activity across different sessions or sites. When combined with form inputs, login activity, or third-party enrichment, fingerprinting can contribute to broader profiling of a user's interests, affiliations, or behaviors.

77. When combined with additional tracking mechanisms such as cookies, login data, and third-party enrichment services, fingerprinting contributes to user profiling. This may include inferring location, browsing habits, consumer preferences, and potentially associating these patterns with known user identities. A sufficiently detailed digital fingerprint especially when correlated with other identifiers such as email addresses, form submissions, or third-party databases, can enable the reidentification of a user.

78. The ability to associate a persistent digital profile with a specific individual using techniques such as digital fingerprinting has led to the development of a data industry known as identity resolution. Identity resolution involves recognizing users across sessions, devices, and platforms by connecting various identifiers derived from their digital behavior, including IP addresses, browser metadata, cookies, and, in some cases, login credentials. The process may occur deterministically (based on known logins or user-submitted information) or probabilistically (based on behavioral or technical similarity).

79. In simpler terms, pen register and trap and trace mechanisms, in the digital context, refer to technologies that record metadata such as IP addresses, URLs visited, and device characteristics, information that identifies the routing and addressing of

electronic communications. This can be achieved through the deployment of tracking technologies like the Trackers installed, executed, embedded, or injected in the Website, which operate without user interaction or visibility.

80. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website when they visited the Website and from when they visited other websites that included the pen register and trap and trace devices.

81. When users visit the Website, installed, executed, embedded or injected Trackers initiate network requests to third-party servers, using invisible image pixels, JavaScript calls, or beacon APIs. These requests include the user's IP address, which is transmitted automatically as part of the HTTP request header. In many cases, the Tracker's server responds by placing a persistent cookie in the user's browser, which serves as a unique identifier that can be used to recognize and track the user across future visits. If a user deletes their browser cookies, this identifier is removed. However, upon revisiting the Website, the process repeats: the browser executes the Tracker's script, a new identifier is set, and the Tracker resumes collecting the user's IP address and associated behavioral data.

D. Plaintiff and Class Members' Data Has Financial Value

82. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data." [23]

83. Consumers' web browsing histories have an economic value of more than $52 per year, while their contact information is worth at least $4.20 per year, and their demographic information is worth at least $3.00 per year. [24]

/ / /

[23] Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct 19, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444.

[24] *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal. 2015), rev'd, 956 F.3rd 589 (9th Cir. 2020).

84. There is a "a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories."[25]

85. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[26]

86. In 2013, the Organization for Economic Cooperation and Development ("OECD") estimated that data trafficking markets had begun pricing personal data, including those obtained in illicit ways without personal consent. It found that illegal markets in personal data valued each credit cardholder record at between 1 and 30 U.S. dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data brokers sell customer profiles of the sort that an online retailer might collect and maintain for about 55 U.S. dollars, and that individual points of personal data ranged in price from $0.50 cents for an address, $2 for a birthday, $8 for a social security number, $3 for a driver's license number, and $35 for a military record (which includes a birth date, an identification number, a career assignment, height, weight, and other information). Experiments asking individuals in the United States and elsewhere how much they value their personal data points result in estimates of up to $6 for purchasing activity, and $150-240 per credit card number or social security number.[27]

/ / /

---

[25] *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3rd 589, 600.

[26] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data.

[27] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), at 27-28, https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

87. The last estimate probably reflects public reporting that identify theft affecting a credit card number or social security number can result in financial losses of up to $10,200 per victim. [28]

88. Data harvesting is one of the fastest growing industries in the country, with estimates suggesting that internet companies earned $202 per American user in 2018 from mining and selling data. That figure is expected to increase with estimates for 2022 as high as $434 per use, reflecting a more than $200 billion industry.

89. The Defendant's monetization of personal data constitutes actionable economic harm under federal law, even without evidence of a direct financial loss, as a "misappropriation-like injury" caused by converting user data into a revenue stream through targeted advertising. In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020).

E. Defendant Is Motivated To Monetize Consumer Information Regardless of Consent

90. By implementing Trackers on the Website, Defendant participates in building detailed behavioral profiles of visitors. These profiles include information such as which users viewed specific products, whether they initiated but abandoned the checkout process, and what pages or buttons they interacted with. This data enables Defendant and its advertising partners to identify repeat visits from the same device or browser. This behavioral data is integrated into third-party advertising platforms, allowing Defendant to deliver retargeted ads to users who previously visited the Website, offer promotional incentives to users who showed purchase intent, and build "lookalike audiences" that target users with similar behaviors or characteristics. These practices significantly improve advertising efficiency and increase the likelihood of converting user engagement into actual sales.

[28] Bradley J. Fikes, Identity Theft Hits Millions, Report Says, San Diego Union Tribune, Sept. 4, 2003, https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html.

91. Defendant has a strong financial incentive to deploy the Trackers on its Website without obtaining user consent. By enabling the collection of IP addresses and device-level identifiers through these technologies, Defendant facilitates integration into real-time bidding ecosystems. These systems rely on bidstream data such as IP address, device type, screen resolution, and referral information to assess the value of a potential ad impression. This enables Defendant and its partners to participate in data-driven ad targeting, increase the value of its advertising inventory, and track users across sessions and websites, all of which provide economic benefit despite the privacy implications to users.

92. IP addresses are a valuable data point in digital advertising and tracking systems. They can be used to approximate a user's geographic location, often down to the city or ZIP code level, enabling location-based targeting. When combined with cookies, browser metadata, and device identifiers, IP addresses contribute to persistent user tracking across sessions and websites. They also assist advertisers and data brokers in linking anonymous browsing activity to existing user profiles, which enhances ad targeting precision and increases the commercial value of each tracked interaction. IP addresses therefore constitute "routing, addressing, or signaling information" protected under CIPA § 638.50(b).

93. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data brokers and ad tech firms aggregate and correlate identifiers such as IP addresses, device IDs, and cookies with other personal data to construct detailed consumer profiles. Information initially gathered in one context, such as browsing a retail website, is frequently repurposed for unrelated uses and sold to third parties without the user's awareness. This results in pervasive surveillance, where users are continuously tracked across multiple websites, applications, and devices, often without their knowledge or ability to opt out.

/ / /

F. Defendant's Conduct Constitutes An Invasion of Plaintiff's and Class Members' Privacy

94. The collection of Plaintiff's and Class Members' personally identifying, de-anonymized information through Defendant's installation and use of the Trackers constitutes an invasion of privacy.

95. As alleged herein, the Trackers are designed to conduct targeted advertising and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' personal information.

96. To put the invasiveness of Defendant's violations of the CIPA into perspective, it is also important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

97. In short, the import of these concepts is that: (i) the Third Parties are data brokers (or partner with data brokers) that collect user information from Website visitors to uniquely identify and de-anonymize users by combining their IP addresses, Device Metadata, User Information, and unique user ID values with whatever information those Third Parties have on a user from other sources; (ii) the Third Parties share that information with other entities to create the most complete user profile they can (through cookie syncing), which includes a more complete and non-anonymous portrait of the user; and (iii) those profiles are offered up for sale through the real-time bidding process to the benefit of Defendant and the Third Parties and to the detriment of users' privacy interests.

/ / /

/ / /

/ / /

/ / /

1. Data Brokers and Real-Timing Bidding: The Information Economy

Data Brokers

98. While "[t]here is no single, agreed-upon definition of data brokers in United States law," [29] California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [i.e., consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

99. Any entity that qualifies as a "data broker" under California law must specifically register as such Cal. Civ. Code § 1798.99.82(a). The Comscore, Nielsen and Magnite trackers employed by Defendant on the Website are operated by registered California data brokers.

100. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties." [30] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data." [31]

/ / /

[29] JUSTIN SHERMAN, DUKE SANFORD CYBER POLICY PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY, at 2 (DUKE SANFORD CYBER POLICY PROGRAM, 2021), https://tinyurl.com/hy9fewhs.

[30] SHERMAN, *supra*, at 2.

[31] Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

101. For instance, the NATO report noted that data brokers collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from observed data by modelling or profiling," meaning what users may be expected to do. On top of this, "[b]rokers typically collect not only what they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use." [32]

102. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals." [33] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees." [34]

103. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations." [35]

104. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data

[32] TWETMAN & BERGMANIS-KORATS, *supra*, at 11.
[33] SHERMAN, *supra*, at 1.
[34] *Id.*
[35] *Id.* at 9.

> (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.
>
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.
>
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups. [36]

105. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving users of the right to control who does and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks. [37]

/ / /

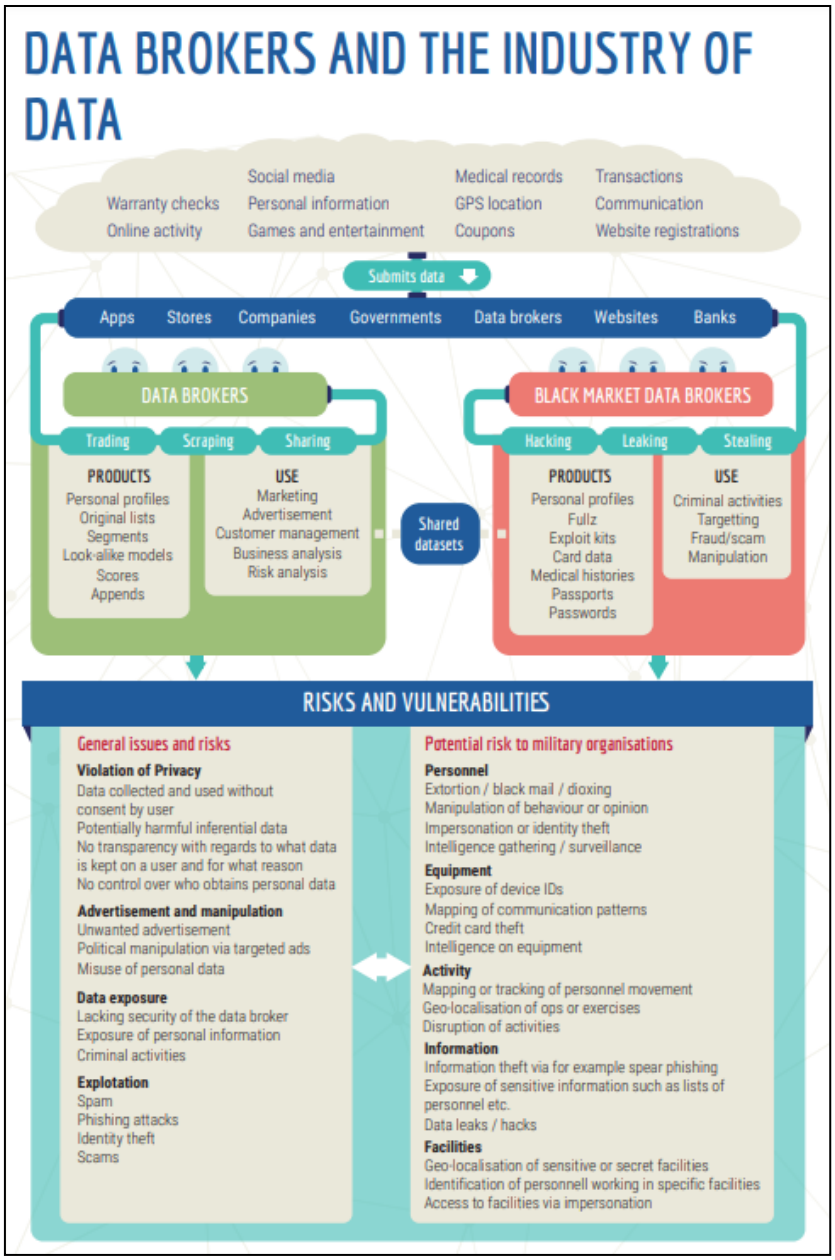
/ / /

/ / /

[36] *Id.*

[37] TWETMAN & BERGMANIS-KORATS, *supra*, at 8.

Figure 4:



106. As noted above, data brokers are able to compile such wide swaths of information in part by collecting users' IP addresses, Device Metadata, and User Information, which is used by data brokers to track users across the Internet. [38]

/ / /

[38] *Id.* at 11.

107. Indeed, as McAfee (a data security company) notes, "data brokers can … even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit." [39]

108. These data brokers will then:

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income. [40]

109. In short, by collecting IP addresses, Device Metadata, and User Information, data brokers and many of the entities the Third Parties sync with can track users across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below.

110. As a result of Defendant's installation of trackers operated by data brokers such as Comscore, Nielsen and Magnite, together with numerous third parties with which those brokers synchronize, the information of Plaintiff and Class Members is appended to existing profiles maintained by those brokers or used to generate new ones. This linkage is accomplished through the collection of IP addresses, device metadata, and other user information transmitted by the browsers of Defendant's Website visitors.

111. These profiles are then served up to any companies that want to advertise on Defendant's Website, and Defendant's users become more valuable as a result of

[39] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

[40] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

having their IP addresses, Device Metadata, and User Information linked to these data broker profiles. Thus, Defendant is unjustly enriched through advertising revenue by installing the Trackers on Plaintiff's and Class Members' browsers, and thus, enabling the Third Parties to collect Plaintiff's and Class Members' IP addresses, Device Metadata, and User Information without consent.

Real-Time Bidding

112. Once data brokers and many of the entities the Third Parties sync with collect Website users' IP addresses, Device Metadata, and User Information, how do they "sell" or otherwise help Defendant monetize that information? This is where real-time bidding comes in.

113. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application." [41]

114. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP work[s] with website or app publishers to help them participate in the RTB process." "DSPs primarily work with advertisers to help them "[r]each relevant audiences on the open internet, drive growth, and prove your impact." [42] And an Advertising Exchange "allows advertisers and publishers to use the same technological platform, services, and methods, and 'speak the same language' in order to exchange data, set prices, and ultimately serve an ad." [43]

/ / /

[41] Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.
[42] *Id.*
[43] *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

115. In other words, SSPs provide user information to advertisers that might be interested in those users, DSPs help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

116. The RTB process works as follows:

> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs [here, *e.g.*, DoubleClick]. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[44]

/ / /

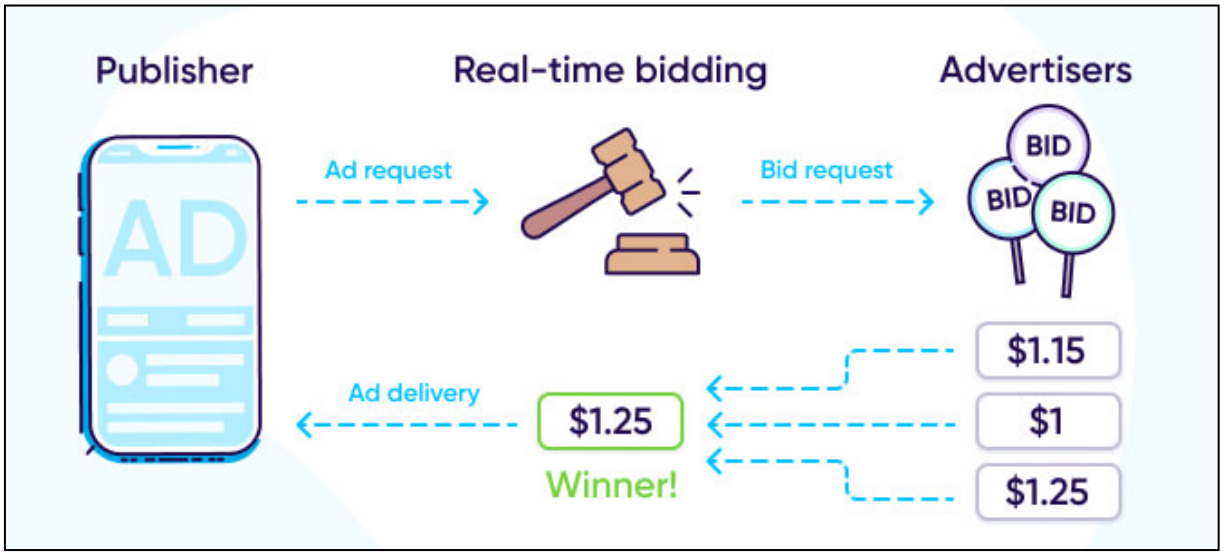
/ / /

/ / /

/ / /

[44] Geoghegan, *supra*; *see also* REAL-TIME BIDDING, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/.

Figure 5:

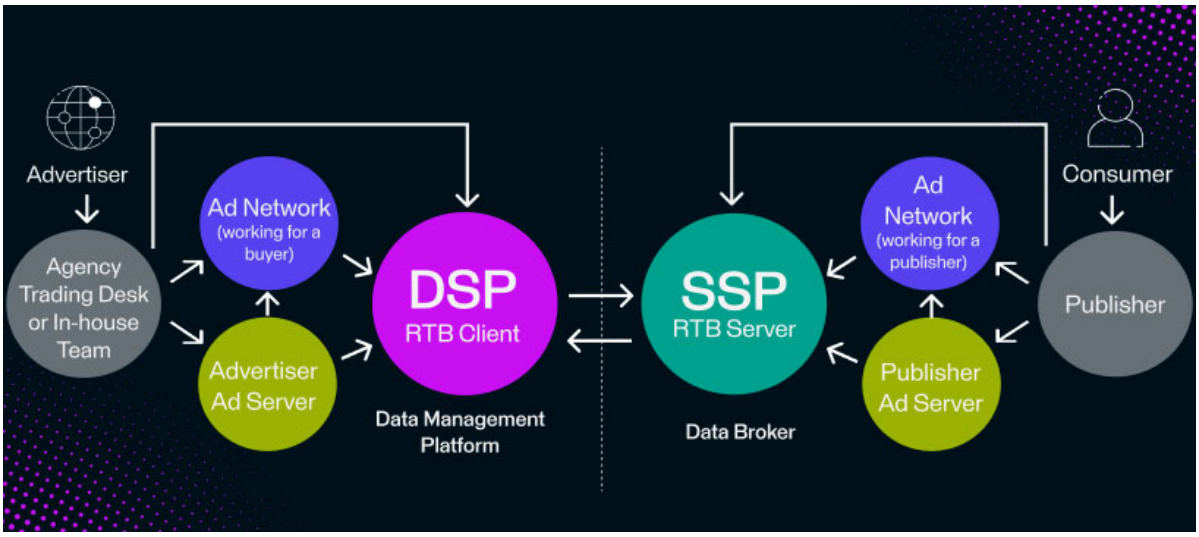


117. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about Defendant's users to procure the greatest interest from advertisers and the highest bids. These entities receive assistance because Defendant also installs the trackers of data brokers on its users' browsers:

> the economic incentives of an auction mean that DSP [or SSP] with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [or a data broker]. DSPs [or SSPs] send bid requests to DMPs [and data brokers], who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers. The DSP with the highest bid not only wins the right to deliver the ad—through the SSP—to the individual. The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.[45]

[45] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022) https://tinyurl.com/yjddt5ey.

Figure 6:



118. In other words, SSPs can solicit the highest bids for Website users by identifying and de-anonymizing those users by combining the information they know about that user with the information other data brokers know about that user. If there is a match, then the SSPs will have significantly more information to provide about users, and that will solicit significantly higher bids from prospective advertisers (because the advertisers will have more information about the user to target their bids).

119. Likewise, a DSP can generate the highest and most targeted bids from advertisers with providing those advertisers with as much information about users as possible, which it does by syncing with data brokers who, in turn, sync with other data brokers and/or are data brokers themselves.

120. All of this naturally enriches Defendant, as its users have now become more valuable thanks to the replete information the Third Parties are able to provide about users.

121. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

a. "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [i.e., Defendant] to share as much end-user data as possible to get higher valuation for their ad

inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."

b. "send[ing] sensitive data across geographic borders."

c. sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[46]

122. The Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[47]

123. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the shear number of entities that receive personal information[48]:

/ / /

/ / /

/ / /

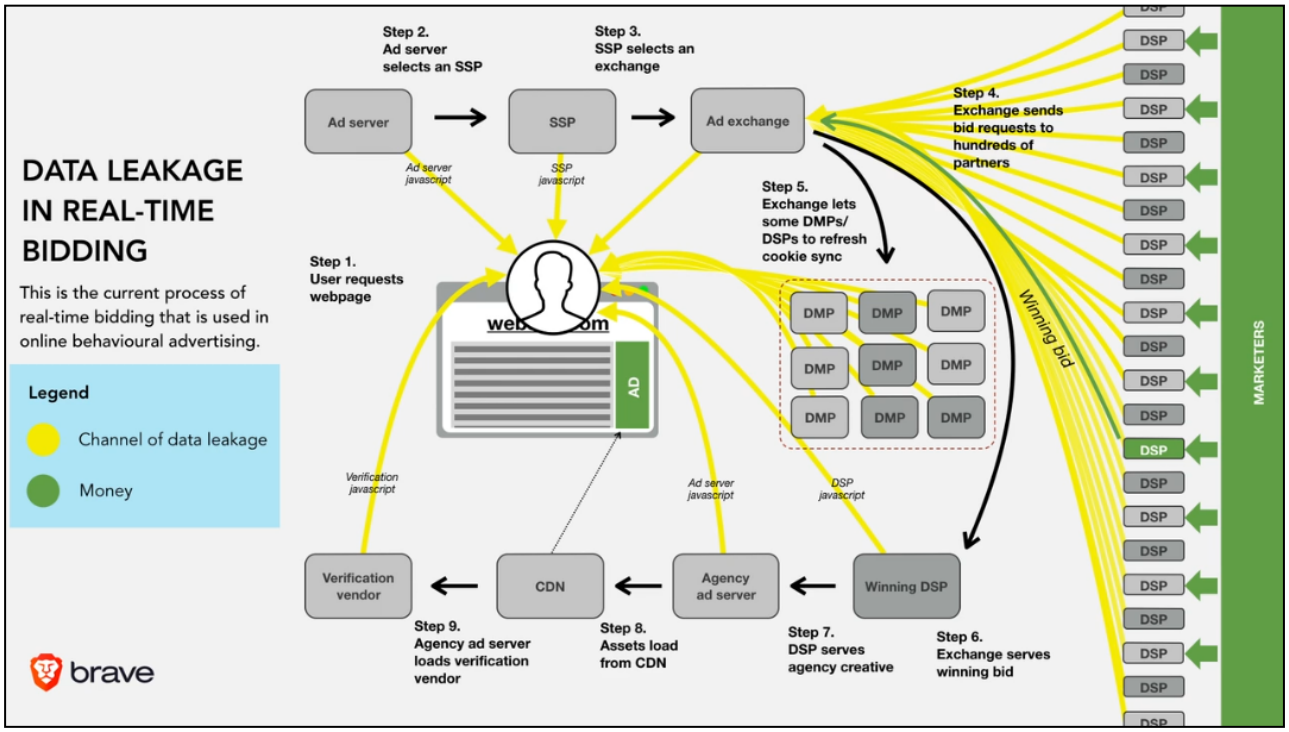
/ / /

[46] FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[47] Geoghegan, *supra*.

[48] DR. JOHNNY RYAN, "RTB" ADTECH & GDPR, https://assortedmaterials.com/rtb-evidence/ (video).

Figure 7:



124. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the CIPA was enacted to protect against. *Ribas v. Clark*, 38 Cal. 3d 355 361 (1985) (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press* 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").'

Cookie Syncing

125. It should should now be clear both the capabilities of the Third Parties (i.e., data brokers, like Comscore, Nielsen and Magnite, who de-anonymize users, or companies who sync with data brokers for this purpose) and the reasons Defendant installs their Trackers on its Website. The final question is how do these Third Parties

share information amongst each other and with others to offer the most complete user profiles up for sale? This occurs through "cookie syncing."

126. Cookie syncing is a process that "allow[s] web companies to share (synchronize) cookies and match the different IDs they assign for the same user while they browse the web."[49] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[50]

127. Cookie syncing ("CSync") works as follows:

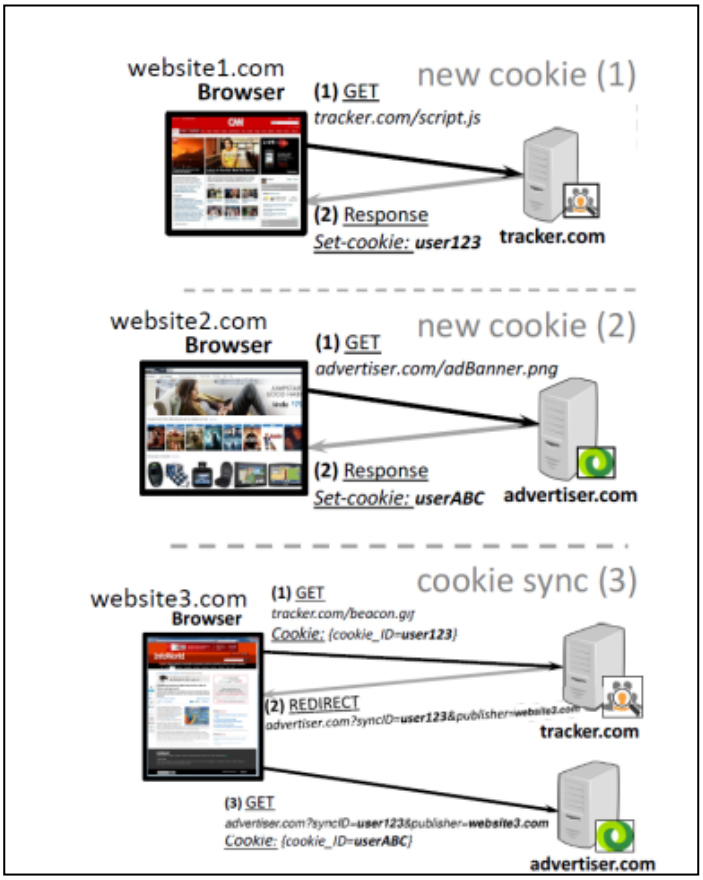
> Let us assume a user browsing several domains like website1.com and website2.com, in which there are 3rd-parties like tracker.com and advertiser.com, respectively. Consequently, these two 3rd-parties have the chance to set their own cookies on the user's browser, in order to re-identify the user in the future. Hence, tracker.com knows the user with the ID user123, and advertiser.com knows the same user with the ID userABC.
>
> Now let us assume that the user lands on a website (say website3.com), which includes some JavaScript code from tracker.com but not from advertiser.com. Thus, advertiser.com does not (and cannot) know which users visit website3.com. However, *as soon as the code of tracker.com is called, a GET request is issued by the browser to tracker.com (step 1), and it responds back with a REDIRECT request (step 2), instructing the user's browser to issue another GET request to its collaborator advertiser.com this time, using a specifically crafted URL (step 3)*.
>
> …
>
> When advertiser.com receives the above request along with the cookie ID userABC, it finds out that userABC visited

[49] Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, 1 WWW '19: THE WORLD WIDE WEB CONFERENCE 1432, 1432 (2019), https://dl.acm.org/doi/10.1145/3308558.3313542.

[50] Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, 6B CCS'14: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674, 674 (2014).

website3.com. *To make matters worse, advertiser.com also learns that the user whom tracker.com knows as user123, and the user userABC is basically one and the same user.* Effectively, CSync enabled advertiser.com to collaborate with tracker.com, in order to: (i) find out which users visit website3.com, and (ii) *synchronize (i.e., join) two different identities (cookies) of the same user on the web.*[51]

Figure 8:



128. Through this process, third party trackers are not only able to resolve user identities (e.g., learning that who Third Party #1 knew as "userABC" and Third Party #2 knew as "user123" are the same person), they can "track a user to a much larger number of websites," even though that "do not have any collaboration with" the third party. [52]

/ / /

[51] Papadopoulos, *supra*, at 1433.
[52] Papadopoulos, *supra*, at 1434.

129. On the flip side, "CSync may re-identify web users even after they delete their cookies."[53] "[W]hen a user erases her browser state and restarts browsing, trackers usually place and sync a new set of userIDs, and eventually reconstruct a new browsing history."[54] But if a tracker can "respawn" its cookie or link to another persistent identifier (like an IP address), "then through CSync, all of them can link the user's browsing histories from before and after her state erasure. Consequently: (i) users are not able to abolish their assigned userIDs even after carefully erasing their set cookies, and (ii) trackers are enabled to link user's history across state resets."[55]

130. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[56]

131. Cookie syncing is precisely what is happening here. When each of the Trackers are installed on Website users' browsers, they are calling and/or syncing their cookies with other third parties on the Website. The result of this process is not only that a single user is identified as one person by these multiple third parties, but they share all of the information about that user with one another (because the cookie is linked to a specific user profile). This prevents users from being anonymous when they visit the Website.

132. To summarize the proceeding allegations, data brokers focus on collecting as much information about Website users as possible to create comprehensive user profiles, and the Trackers sync with numerous other data brokers that do the same. The Third Parties collect IP addresses, Device Metadata, User Information, and unique user IDs in the first instance, but those pieces of information are connected to information the Third Parties glean from other sources (e.g., various data brokers) to build comprehensive profiles. Through "cookie syncing," those profiles are shared amongst

---

[53] *Id.*
[54] *See id.*
[55] *Id.*
[56] *Id.* at 1441.

the Third Parties and with other entities to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to interested advertisers through real-time bidding using the Third Parties' trackers, where users will command more value the more advertisers know about a user.

133. Thus, the Third Parties enrich the value Defendant's users would otherwise command by tying the data they obtain directly from users on the Website (e.g., IP addresses, Device Metadata, User Information, unique user IDs) with comprehensive user profiles.

134. Accordingly, Defendant is using the Trackers in conjunction with the Third Parties to (i) de-anonymize users, (ii) offer its users up for sale in real-time bidding, and (iii) monetize its Website by installing the Trackers and allowing the Third Parties to collect as much information about Website users as possible (without consent).

135. Thus, Defendant is unjustly enriched through their installation and use of the Trackers, which causes data to be collected by Third Parties without Plaintiff's and Class Members' consent, and that enable the Third Parties to sell Defendant's user inventory in an ad-buying system. In addition, Plaintiff and Class Members lose the ability to control their information, as their information ends up in the hands of data brokers, advertising inventory sellers, and a virtually unlimited number advertisers themselves without knowledge or consent.

136. When a user visits the Website, a suite of background tracking technologies is activated immediately upon page load. These include client-side scripts deployed by third-party Trackers, which begin collecting various categories of User Information without any visible indication to the user. Together, these technologies function as a coordinated data collection infrastructure that allows Defendant to analyze user behavior at a highly granular level and to leverage that insight in real time for marketing optimization, user targeting, and business intelligence.

137. On information and belief, the Trackers operate as part of a vast and interconnected digital advertising ecosystem and these entities leverage shared

identifiers, cookie syncing, and cross-device tracking techniques to follow users across websites, platforms, and environments, with tools specifically engineered to build persistent consumer profiles, enabling real-time behavioral targeting and identity resolution at scale.

138. Defendant deploys the Trackers to build a behavioral profiling and targeted advertising system. Several of these trackers are dynamically injected into the Website through tag management systems, initiating the collection of user behavior such as pageviews, navigation patterns, and session metadata. Others are directly embedded into the Website's code, firing automatically upon page load. Together, these technologies associate user behavior with device identifiers, cookies, and pseudonymous advertising IDs, facilitating the construction of persistent user profiles for advertising and marketing purposes.

139. The Trackers participate in programmatic advertising ecosystems by capturing behavioral signals from the Website and linking them to advertising audiences. These trackers enable personalized ad delivery based on users' site interactions and associate browsing activity with broader ad networks through identifier syncing. Each of these platforms sets or reads cookies to maintain persistent tracking across sessions and domains, effectively participating in workflows designed to reidentify users and expand behavioral audience segments for targeted advertising.

G. Defendant Shared Plaintiff's Personal Behavioral Data With Third Parties

140. The third-party recipients of Plaintiff's transmitted data included several advertising, analytics, auction, and measurement companies whose code Defendant embedded into the Website. Among these was Google, whose advertising and measurement infrastructure served through domains such as securepubads.g.doubleclick.net, pagead2.googlesyndication.com, googleads.g.doubleclick.net, s0.2mdn.net, and googletagmanager.com, received the full ESPN homepage URL, referrer values, session-linking identifiers, and ad-slot context

information associated with Plaintiff's visit. These parameters allowed Google's systems to identify the specific page Plaintiff accessed, the homepage advertising units rendered during the session, and the device characteristics reflected in the User-Agent metadata transmitted with each request.

141. Plaintiff's device also communicated with Magnite, the operator of fastlane.rubiconproject.com, prebid-a.rubiconproject.com, and micro.rubiconproject.com, which function as part of the Website's header-bidding and real-time auction framework. The transmissions to these domains included bidder-context signals, ad-slot identifiers, and homepage-specific placement information, enabling Magnite to evaluate or price the advertising inventory presented to Plaintiff during her session. A similar set of disclosures occurred in communications with Xandr through ib.adnxs.com, where the Website transmitted auction-related data and device identifiers that allowed Xandr to participate in real-time bidding on homepage advertising impressions.

142. Additional advertising systems engaged during Plaintiff's visit included Yahoo Ads, through c2shb.pubgw.yahoo.com, which received homepage ad-slot data and device metadata as part of the Website's advertising-delivery sequence. Kargo, operating through krk2.kargo.com, similarly received request parameters reflecting the placement and configuration of the homepage advertising containers and the characteristics of Plaintiff's mobile device, which its platform uses to shape the formatting and delivery of mobile ad creatives. The Website also transmitted homepage advertising and resource-load data to 33Across via cdn-ima.33across.com, enabling that platform to participate in the optimization or delivery of homepage advertising units served to Plaintiff.

143. The Website further disclosed Plaintiff's device information and homepage location to audience-measurement providers. Nielsen, operating through imrworldwide.com domains, received requests containing Plaintiff's User-Agent fields and the homepage URL, allowing its measurement systems to record the device type and

page accessed during the session. Comscore, through scorecardresearch.com and sb.scorecardresearch.com, similarly received the homepage URL, referrer information, and device metadata, enabling its measurement infrastructure to model or classify the visit. Across all of these vendors, the transmitted data included the full homepage URL, referrer headers, device-level identifiers, auction-context parameters, and homepage advertising-slot attributes that were sent only because Defendant embedded these third-party JavaScript frameworks into the Website and caused them to execute on Plaintiff's device.

144. The data transmitted to these third parties was personal and behavioral in nature because it identified the specific webpage Plaintiff accessed, revealed the originating and destination locations of her browsing activity, and exposed detailed information about the device she used to access the Website, including her browser family, operating system characteristics, and mobile-specific identifiers contained in the User-Agent fields. The data also included session-linking identifiers and ad-slot context parameters that reflected Plaintiff's real-time interactions with the Website and the advertising units rendered during her visit. Taken together, this information enabled third-party advertising, auction, measurement, and analytics companies to recognize Plaintiff's device across different sessions, associate the ESPN homepage visit with her broader online activity, and model her behavior for purposes of ad-targeting, measurement, or cross-site profile building. The disclosures therefore conveyed individualized information about who was browsing, what page was being viewed, and how Plaintiff's device interacted with the Website and its advertising systems, constituting personal and behavioral data.

V. SPECIFIC ALLEGATIONS

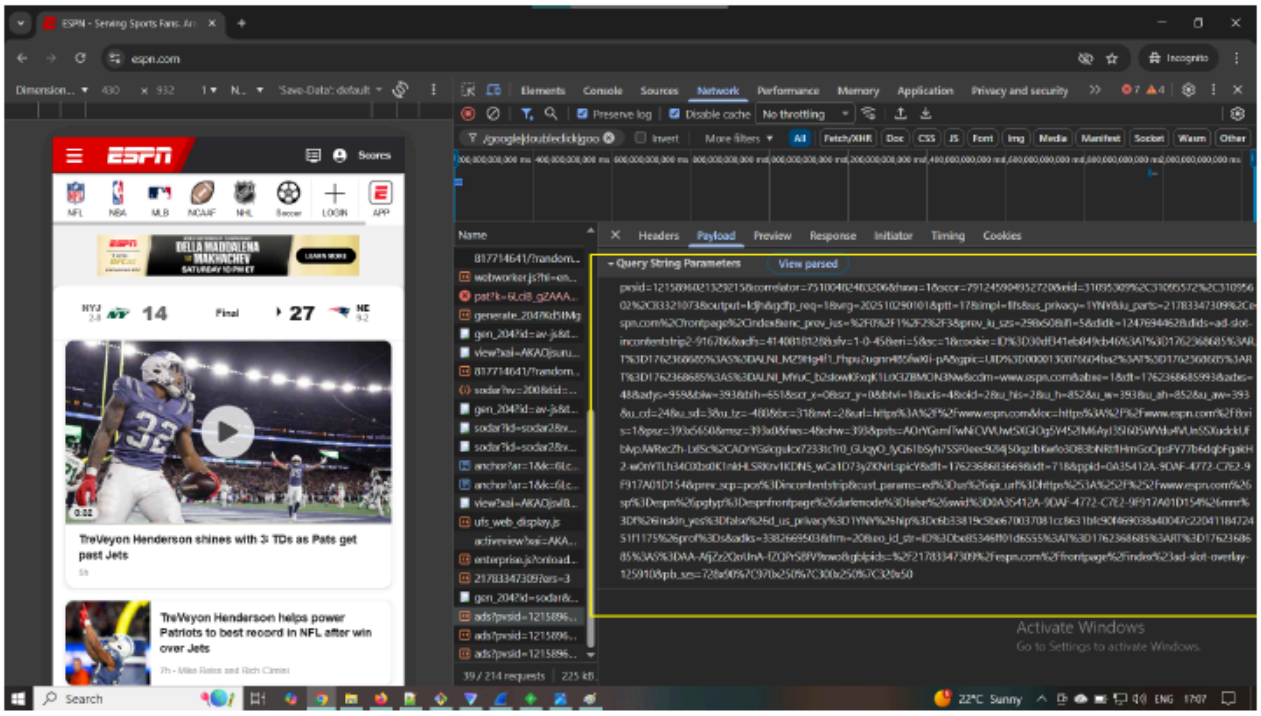
A. Google Ads / DoubleClick / Tag Manager Tracker

145. The Google Ads, DoubleClick, and Tag Manager technologies (collectively, the "Google Tracker") are third-party advertising, measurement, and behavioral-tracking systems operated by Google LLC. When implemented on a website,

these systems load and execute multiple JavaScript resources that cause a user's device to transmit signaling, routing, addressing, device-identification, and behavioral information directly to Google's servers.

146. As shown in Figure 9, immediately upon loading the Website Plaintiff's browser initiated outbound connections to Google's tracking and advertising infrastructure, including requests to googletagmanager.com, googleads.g.doubleclick.net, g.doubleclick.net, and googlesyndication.com. Figure A3 shows that these transmissions occurred automatically at the outset of the session without any interaction or consent from the user because Defendant embedded code that caused Google's tracking endpoints to activate the moment the Website loaded.

Figure 9:

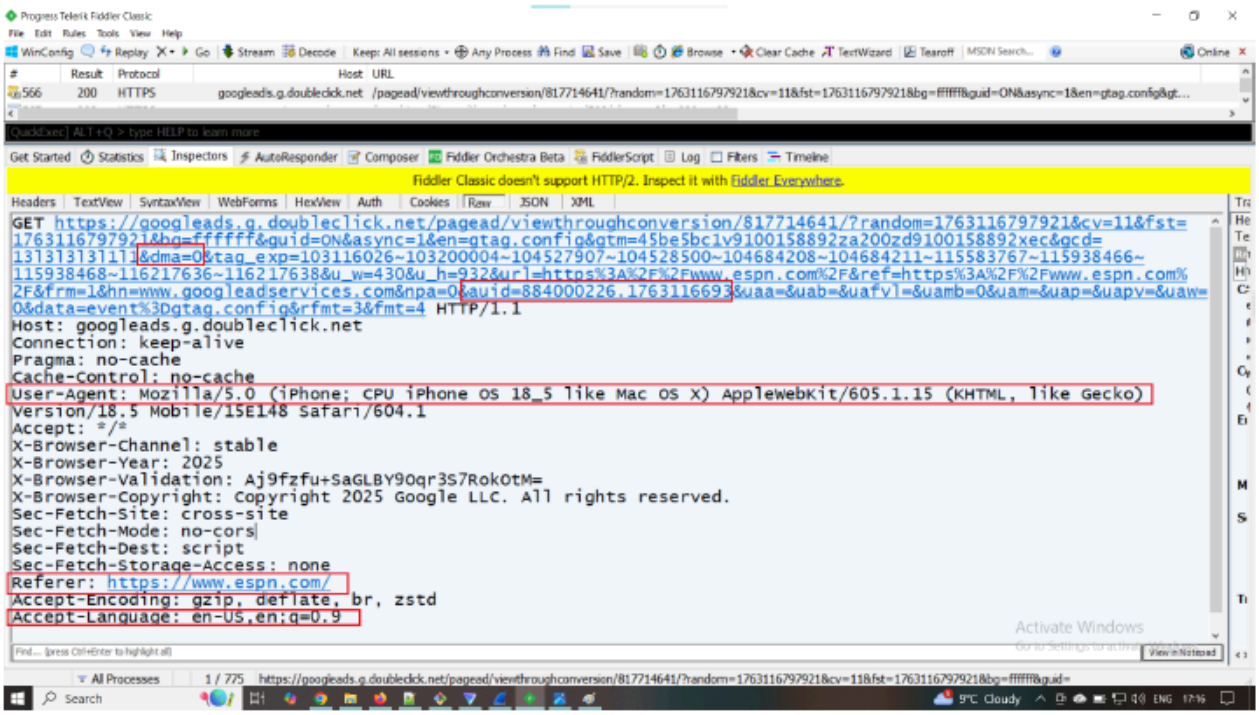


147. Once triggered, the Google Tracker transmitted detailed behavioral, contextual, and device-level metadata about the user's visit. Figure 9 shows unique identifiers (including pvsid and gcl_au), page-location fields identifying the specific ESPN page being viewed, referrer information, session-linking values, advertising-slot parameters, and device fingerprinting attributes contained within the User-Agent string.

These values reveal the nature of the page accessed, the advertising calls rendered during her visit, and the characteristics of the device from which the user accessed the Website.

148. Additional evidence of Google's data collection appears in Figure 10, which shows Google endpoints receiving the user's complete User-Agent string, full page URL, referrer headers, and IP-derived geolocation attributes (including dma). Figure 10 confirms that Google's infrastructure received the user's device and navigation information in clear form, including signals that allow Google to place the user's activity within a geographic region derived from the user's IP address.

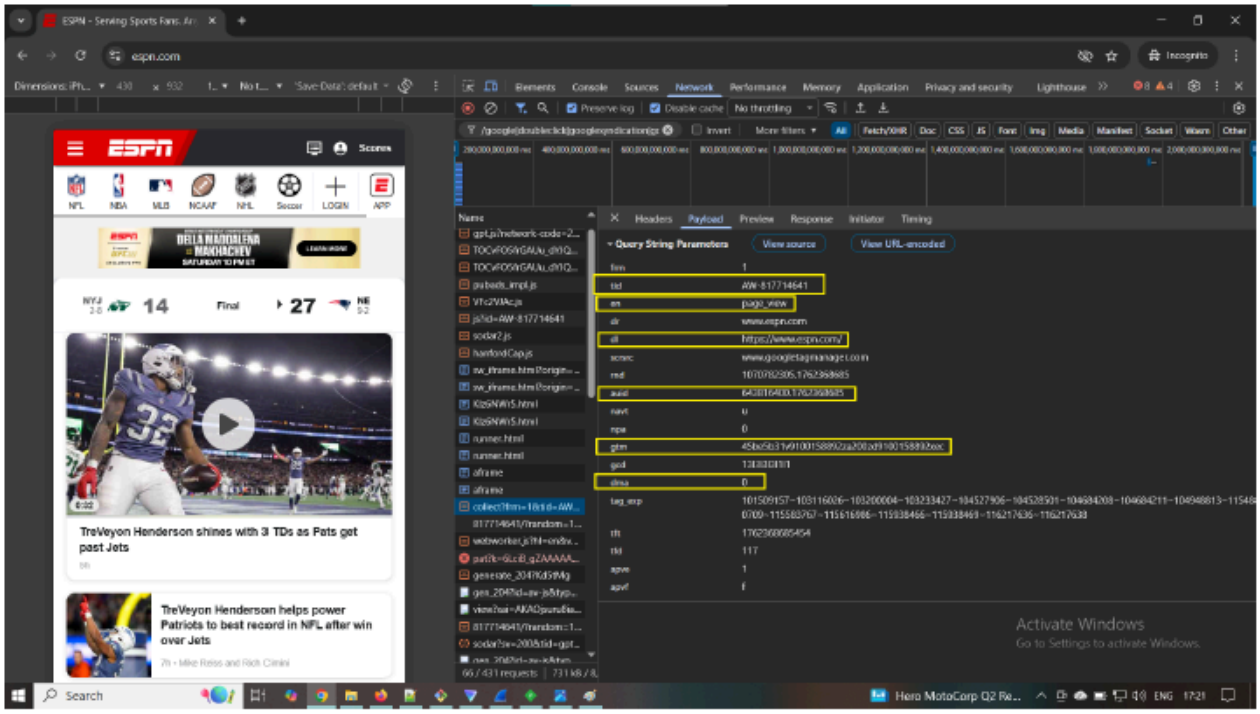
Figure 10:



149. Figure 11 further demonstrates Google's receipt of tracking, advertising, and analytics data generated by the Google Tracker. Figure 11 displays outbound "collect" requests containing page URL parameters (dl), referrer parameters (dr), Google identity tokens (including audid), and additional device and timing attributes that enable Google to recognize the user's device, connect sequential resource loads, and record the specific ESPN content rendered in the user's session.

/ / /

Figure 11:



150. Figure 12 shows the DNS lookup process by which the user's actual source IP address was transmitted as part of the Website's connections to Google's tracking domains. In Figure 12, the user's source IP appears in the DNS requests resolving Google endpoints such as g.doubleclick.net, googleads.g.doubleclick.net, and googletagmanager.com. This constitutes direct evidence that the user's IP address, an identifying, addressing, and routing value, was transmitted to Google's authoritative DNS infrastructure as a result of Defendant's tracking integrations.

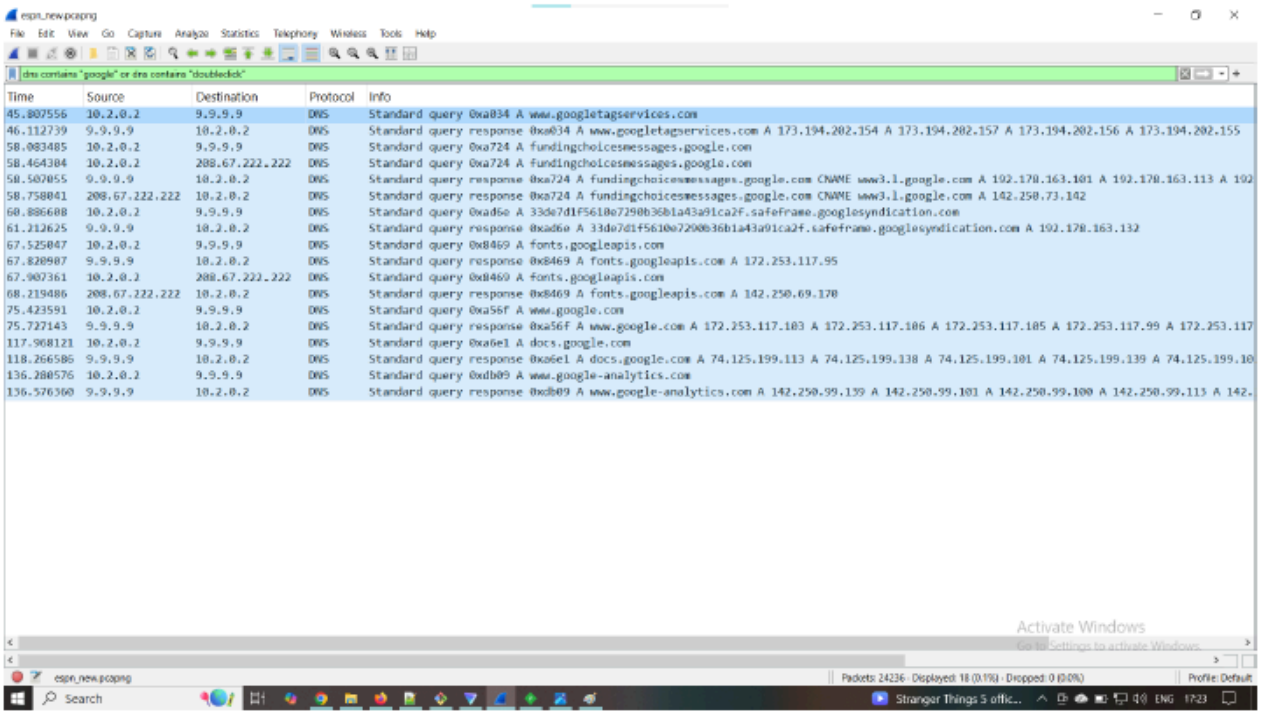
/ / /

/ / /

/ / /

/ / /

Figure 12:



151. Taken together, Figures 9 through 12 establish that Defendant designed the Website to automatically download and execute Google's tracking and advertising scripts, resulting in the transmission of Plaintiff's dialing, routing, addressing, device-identification, behavioral, and page-context information to Google. These transmissions include: (1) the user's source IP address, (2) device fingerprinting attributes, (3) unique Google identifiers, (4) page-location and referrer fields, and (5) advertising-slot and session-linking metadata. All such disclosures occurred automatically and without the user's knowledge or consent.

152. The Google Tracker constitute a "process" because it consists of software and scripts that operate on computing hardware to identify consumers, gather information, and correlate data across sessions. It also constitutes a "device," because it operates as software installed and executed on a user's device to collect information. See *James v. Walt Disney Co.*, 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

153. The Google Tracker functions as a pen register and/or trap-and-trace device under Cal. Penal Code § 638.50 because it captures outgoing metadata including full

page URLs, referrer headers, timestamps, cookies, and advertising identifiers and receive inbound server-address data and set-cookie information. These transmissions constitute the acquisition of addressing, signaling, routing, and device-identification information as defined by § 638.51.

154. Defendant did not obtain a court order authorizing the use of a pen register or trap-and-trace device and did not obtain Plaintiff's or Class Members' consent for the installation or operation of the Google Tracker.

155. By embedding and enabling Google Tracker without user consent or judicial authorization, Defendant violated Cal. Penal Code § 638.51.

B. The Magnite Tracker

156. Rubicon Project (Magnite) operates the Website's supply-side advertising exchange and Prebid auction infrastructure. When embedded on a website, Magnite's scripts load automatically and transmit signaling, routing, addressing, device, and behavioral information to Magnite's servers for real-time bidding, impression valuation, and cross-exchange identity synchronization.

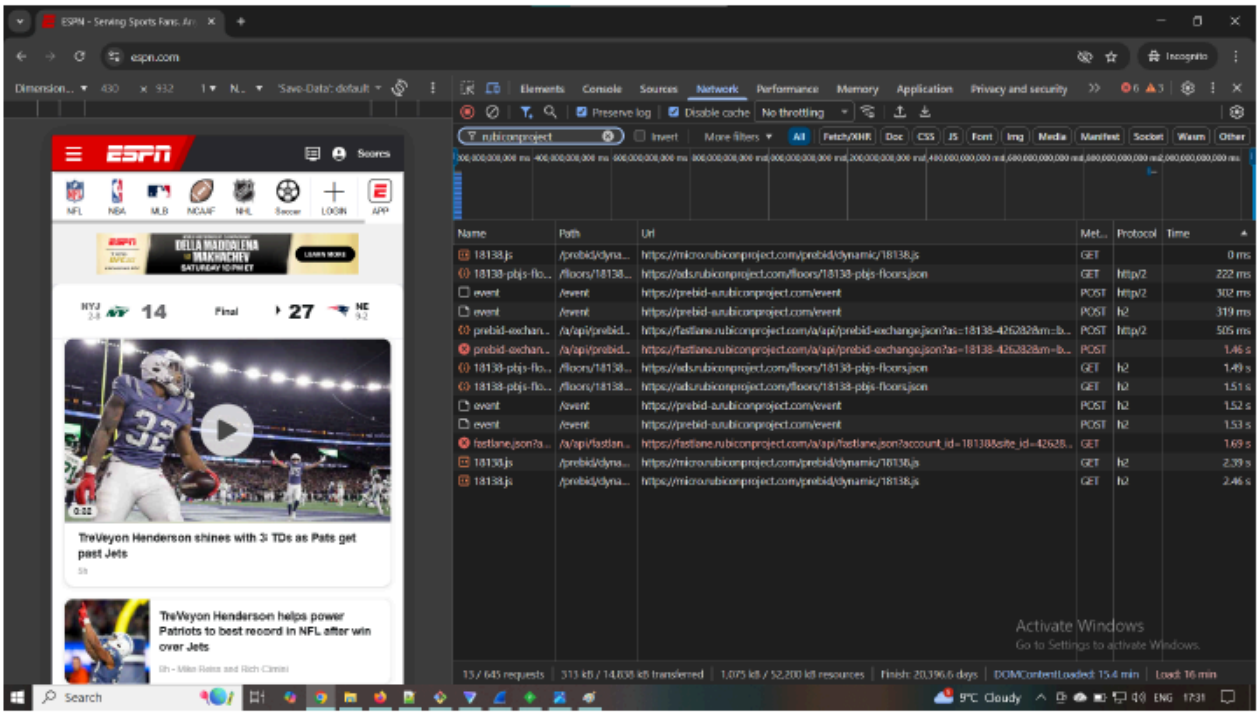
157. As shown in Figure 13, immediately upon loading the Website the browser triggered connections to multiple Magnite endpoints, including micro.rubiconproject.com, ads.rubiconproject.com, fastlane.rubiconproject.com, and prebid-a.rubiconproject.com. These requests executed within milliseconds of navigating to espn.com, confirming that Defendant configured the Website so that Magnite's tracking and bidding systems activate automatically without any user interaction or consent.

/ / /

/ / /

/ / /

Figure 13:



158. Once initialized, the Magnite integration transmitted detailed device, browser, and contextual data. Figure 14 shows Rubicon receiving (1) viewport width and height, (2) renderable area dimensions (vpw, vph), (3) language settings, (4) a full mobile User-Agent string, (5) ESPN's publisher domain and page URL (https://www.espn.com/), and (6) a us_privacy value of "1YNY" indicating no consent. These parameters reflect device fingerprinting, locale identification, and behavioral context, none of which are required for routing or transport but are used by Magnite to segment, classify, and bid on the user's advertising impressions.

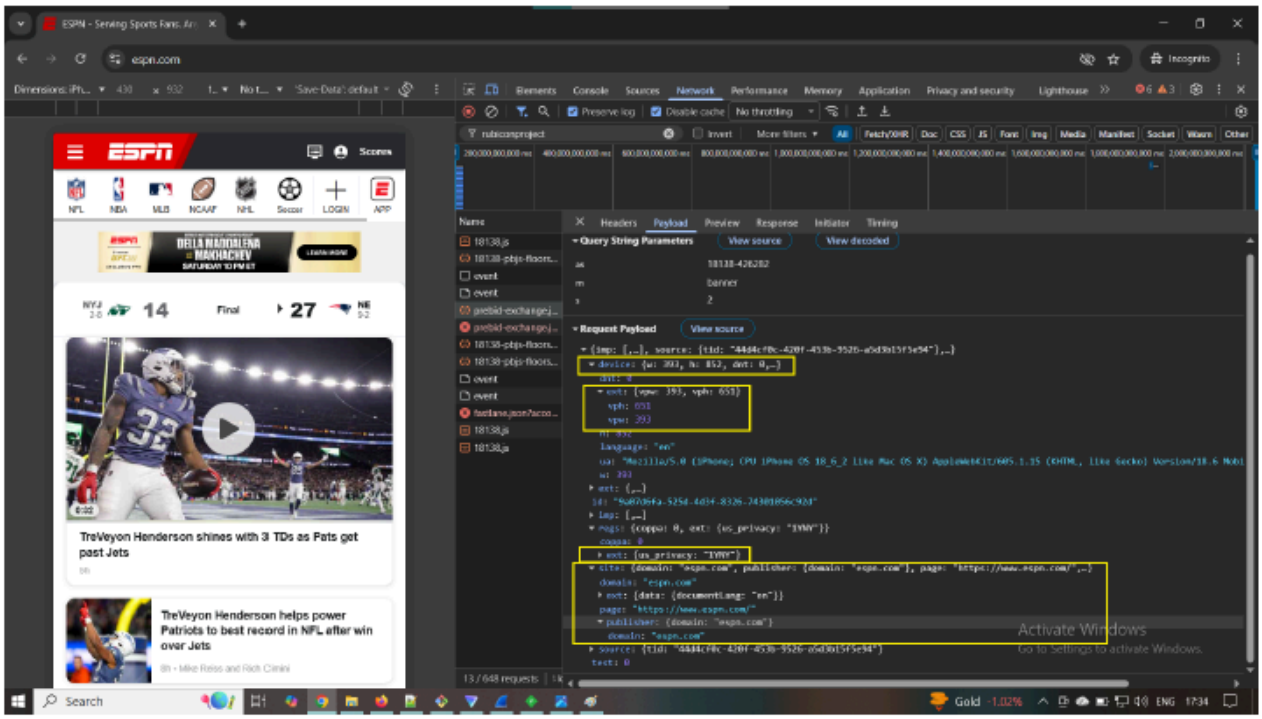
/ / /

/ / /

/ / /

/ / /

Figure 14:



159. Figure 15 captures Magnite's generation and exchange of identity signals during the same session. Magnite created and received a sessionId, a pageview identifier (pvid), an auctionId, and a transactionId, along with adUnitCodes and a bidderOrder list identifying downstream partners (trustx, rubicon, yahoossp, ix, appnexus, kargo). These identifiers allow Rubicon to recognize the visitor within a session, link impressions across auctions, and coordinate with other bidding platforms. Their automatic creation demonstrates intentional identity-acquisition functionality rather than mere transmission of routing information.

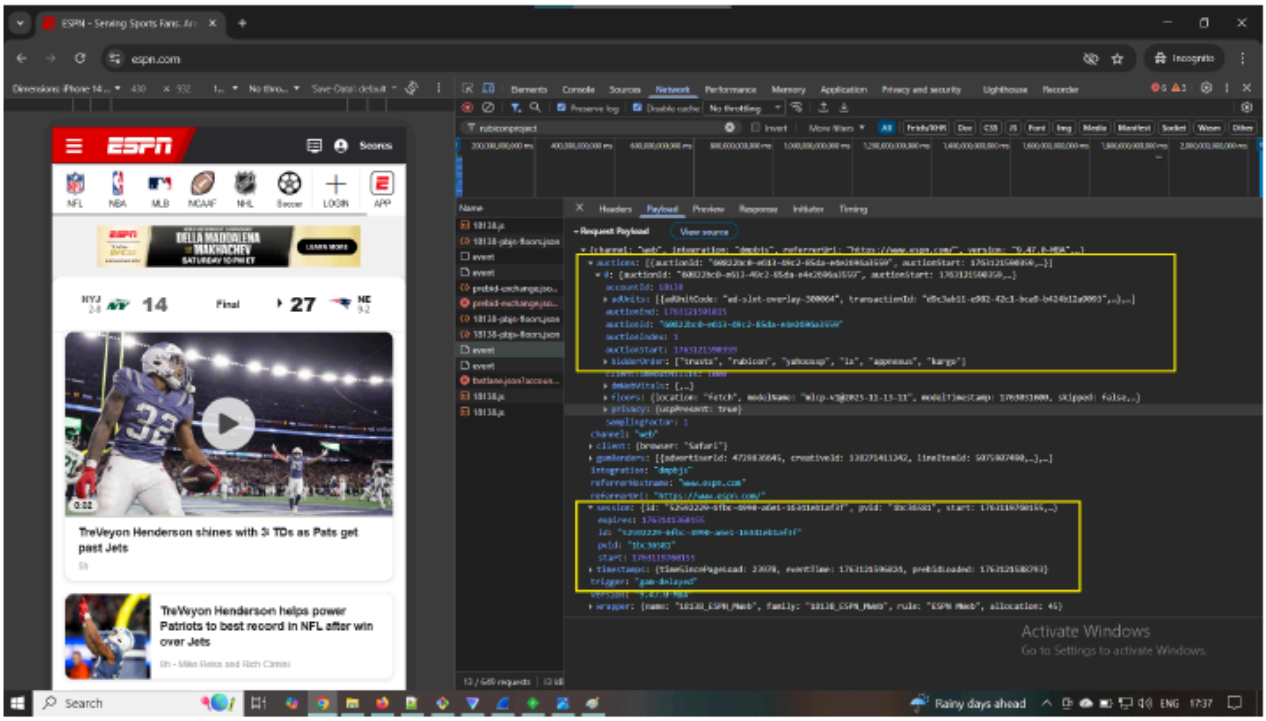
/ / /

/ / /

/ / /

/ / /

Figure 15:



160. Critically, **Figure 16** shows the DNS lookup process in which the client's actual source IP address (10.2.0.2) was transmitted to resolve Magnite domains, including micro.rubiconproject.com, ads.rubiconproject.com, and prebid-a.rubiconproject.com. These DNS requests occurred during the Website's loading sequence and before any consent was displayed, providing direct evidence that Plaintiff's IP-addressing information was sent to Magnite's infrastructure as part of Defendant's tracking and bidding integrations.

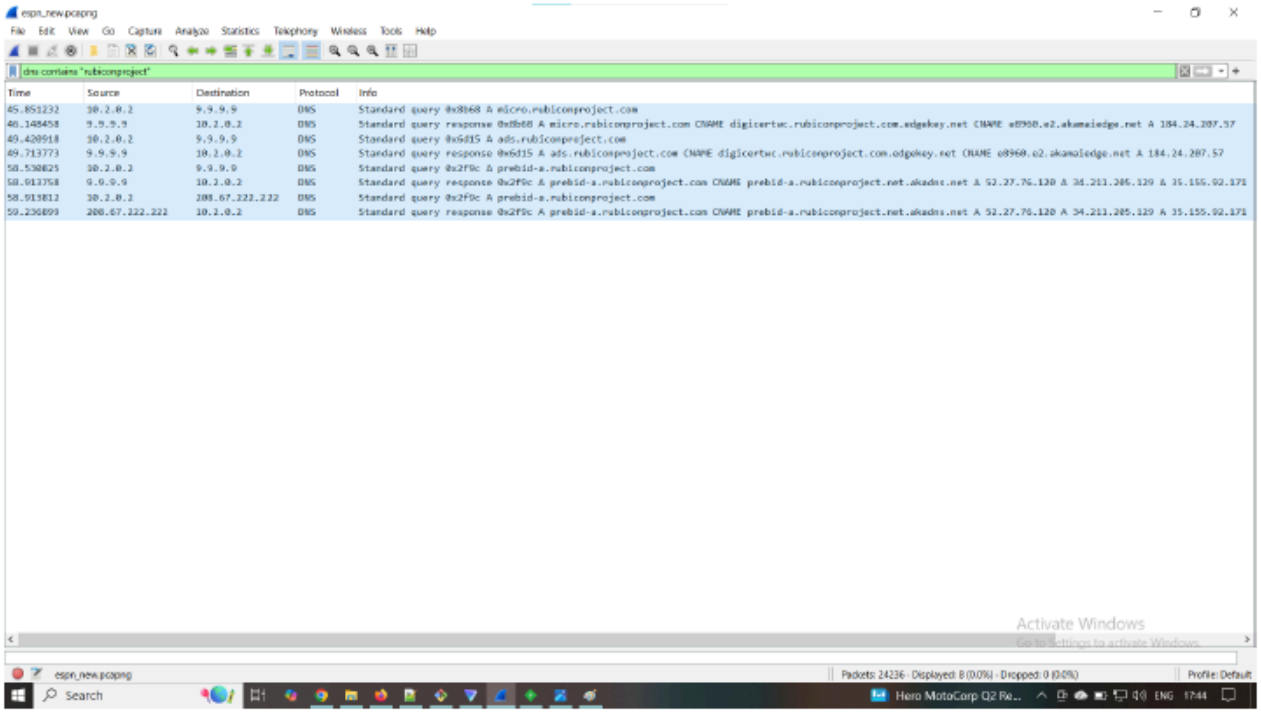
/ / /

/ / /

/ / /

/ / /

Figure 16:



161. Figures13 through 16 collectively establish that Defendant designed the Website to automatically load and execute Magnite's Prebid and exchange scripts, causing the user's device to transmit (1) the source IP address, (2) device fingerprinting attributes, (3) page-context metadata, (4) User-Agent information, (5) consent-state values, and (6) multiple persistent identifiers linking the visit to Rubicon's real-time bidding ecosystem. These transmissions reveal personal behavioral information including the ESPN homepage context associated with the user's visit and identifying signals used by Magnite to track, classify, price, and synchronize impressions across partner platforms.

162. The Magnite tracking and bidding infrastructure constitutes a "process" because it consists of software and scripts that operate on computing hardware to identify consumers, gather information, and correlate that information across requests and auctions. Magnite's integrations function only when their JavaScript code executes on a user's device and collects data describing the user's device, ad-slot context, identity tokens, and session-level metadata. The Magnite codebase also constitutes a "device,"

because it operates through software installed and executed on Plaintiff's device for the purpose of collecting information. See *James v. Walt Disney Co*., 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

163. Magnite's tracking and bidding scripts function as a pen register and/or trap-and-trace device under Cal. Penal Code § 638.50 because they capture outgoing metadata including full page URLs, referrer information, timestamps, device fingerprints, consent-state fields, auction identifiers, and other signaling parameters and receive inbound server-address data, identity tokens, and auction-response metadata, which constitutes the acquisition of "dialing, routing, addressing, and signaling information" within the meaning of § 638.51.

164. Defendant did not obtain a court order authorizing the use of a pen register or trap-and-trace device and did not obtain Plaintiff's or any Class Member's consent for the installation, activation, or operation of the Magnite tracking, bidding, identity-generation, or auction-synchronization scripts at issue.

165. By embedding and enabling Magnite's bidding systems without user consent or judicial authorization, and by causing Plaintiff's device to transmit her IP address, device-fingerprinting data, page-context information, session identifiers, and auction-context metadata to Magnite, Defendant violated Cal. Penal Code § 638.51.

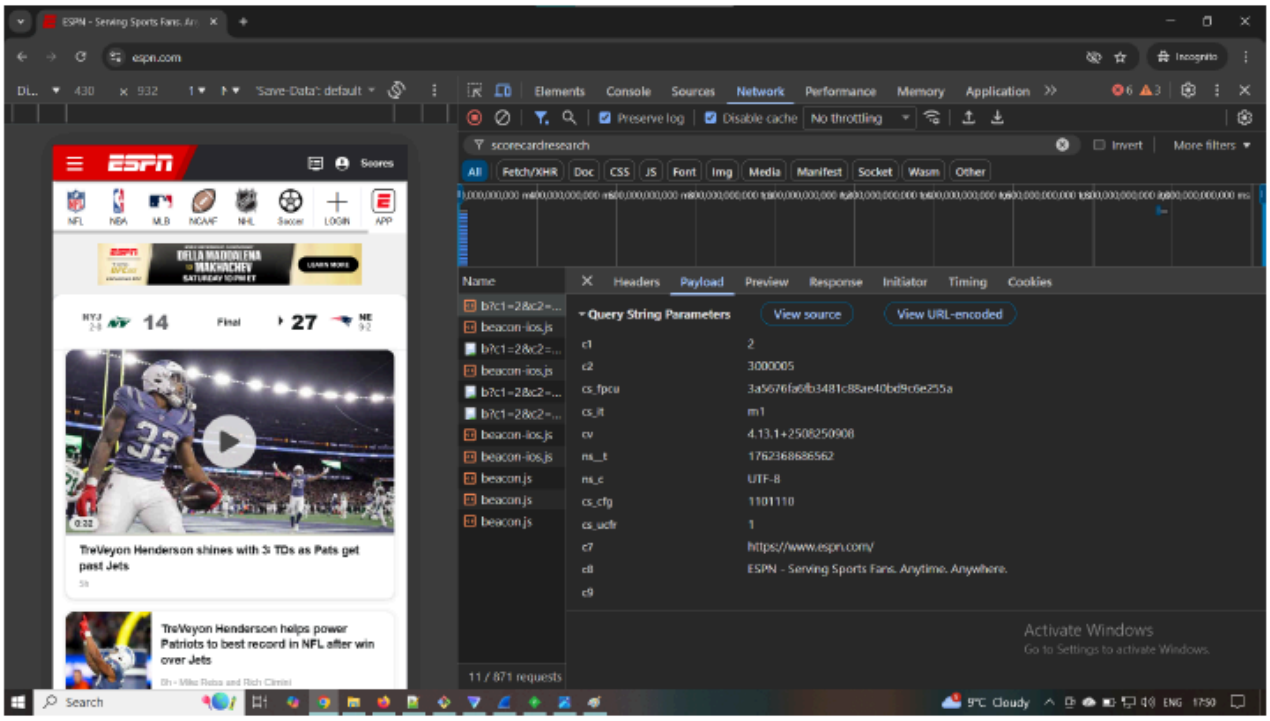
C. The Comscore Tracker

166. Comscore provides the Website's third-party behavioral-measurement and audience-tracking systems through scorecardresearch.com and sb.scorecardresearch.com. These systems function as cross-site tracking technologies that collect signaling, routing, addressing, device, and navigation information whenever a website embeds Comscore's measurement beacons.

167. As shown in Figure 17, the Website caused Comscore's tracking endpoints to activate immediately when the user accessed the page. Without any interaction or consent, Comscore received the full URL of the ESPN page the user visited, referrer information identifying that same page as the source of the request, and session-level

measurement parameters. These fields reveal exactly which ESPN page the user accessed and the navigation context associated with that visit.

Figure 17:



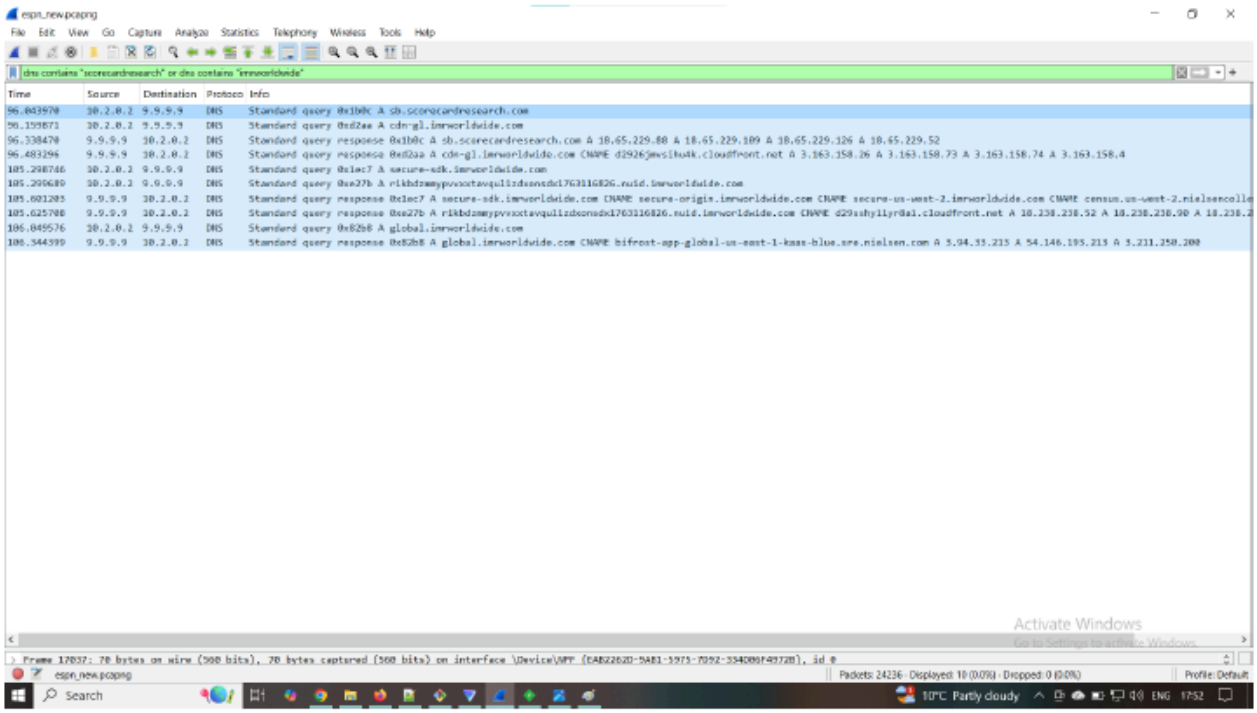
168. Additional evidence of Comscore's data collection appears in Figure 18, which shows Comscore receiving the user's complete User-Agent string, operating-system indicators, browser family, locale, and other device-fingerprinting attributes. These values identify the type of device the user was operating, the software environment running on it, and the technical characteristics of the user's browser—allowing Comscore to classify the user's device and associate the session with Comscore's broader cross-property measurement systems.

/ / /

/ / /

/ / /

Figure 18:



169. Figure 19 captures the DNS resolution process in which the user's source IP address was transmitted to resolve Comscore's tracking domains. The DNS timeline in Figure C6 shows the user's IP address being sent to the authoritative DNS servers for scorecardresearch.com and sb.scorecardresearch.com, confirming that Comscore received the user's dialing, routing, and addressing information as part of the Website's tracking operations.

/ / /

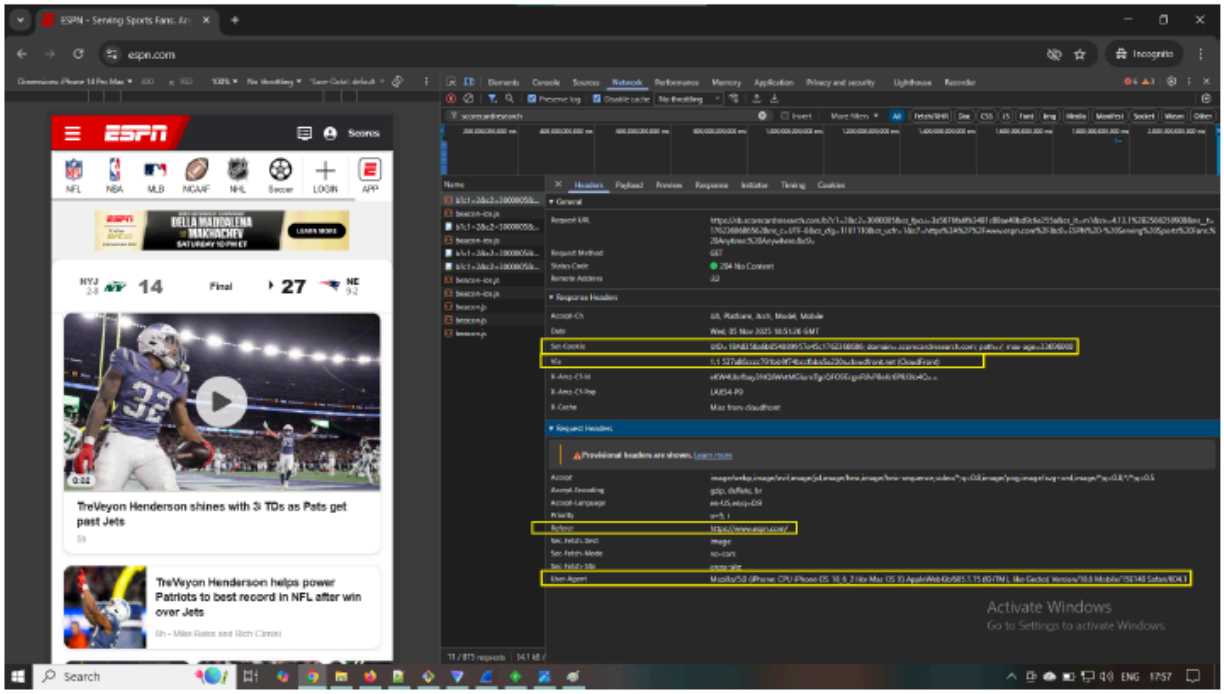
/ / /

/ / /

/ / /

/ / /

Figure 19:



170. Further evidence of Comscore's data collection appears in Figure 20, a real-time HTTP transaction capture generated through Fiddler, which records packet-level request metadata as it leaves the user's device. Figure C5(a) shows that Comscore received the user's full User-Agent string, the ESPN homepage URL, the referrer associated with that page, language settings, operating-system information, and additional device-fingerprinting fields. These packet-level request details confirm that the Website caused the user's browser to transmit uniquely identifying device metadata and specific page-context information directly to Comscore's servers.

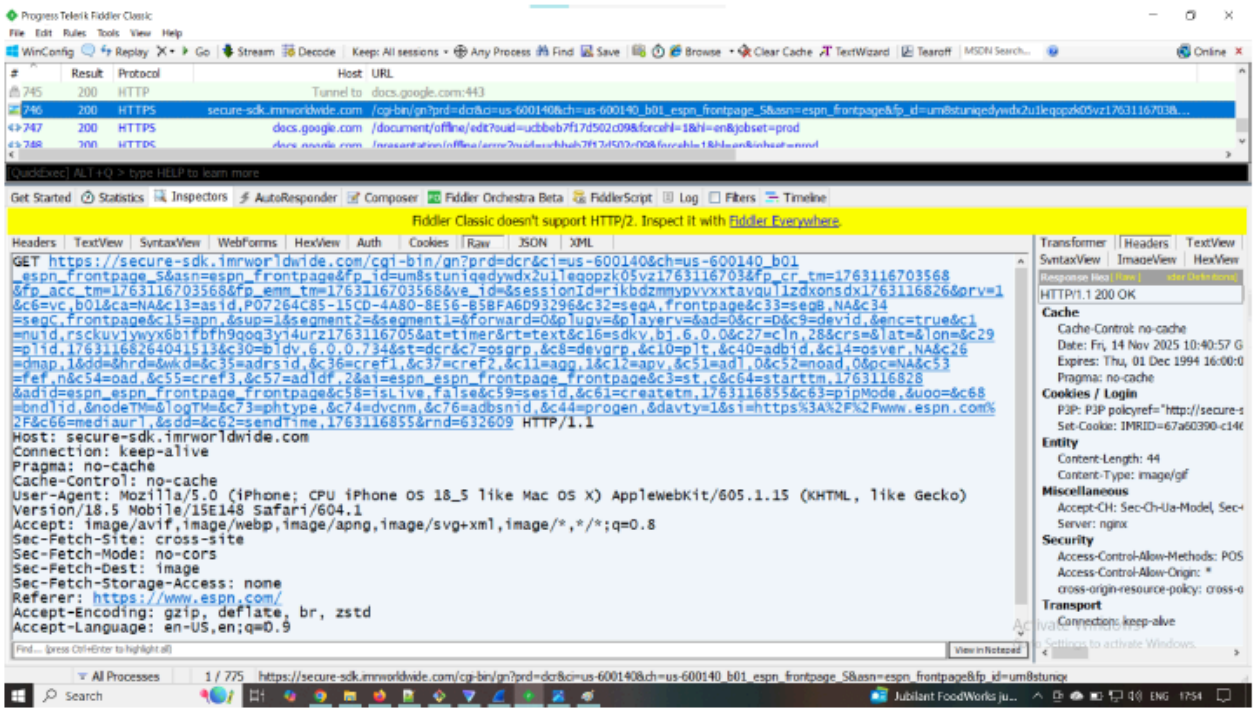
/ / /

/ / /

/ / /

/ / /

Figure 20:



171. Figure 21, also captured through Fiddler, shows the corresponding packet-level HTTP response from Comscore's infrastructure. This response contains Comscore's tracking instructions, measurement tokens, and additional identifiers generated by Comscore's servers as part of the same transaction. The presence of these identifiers in the response confirms a completed two-way exchange between the user's device and Comscore, in which Comscore both received the user's device and navigation metadata and transmitted server-side identifiers back to the user for continued tracking and measurement.

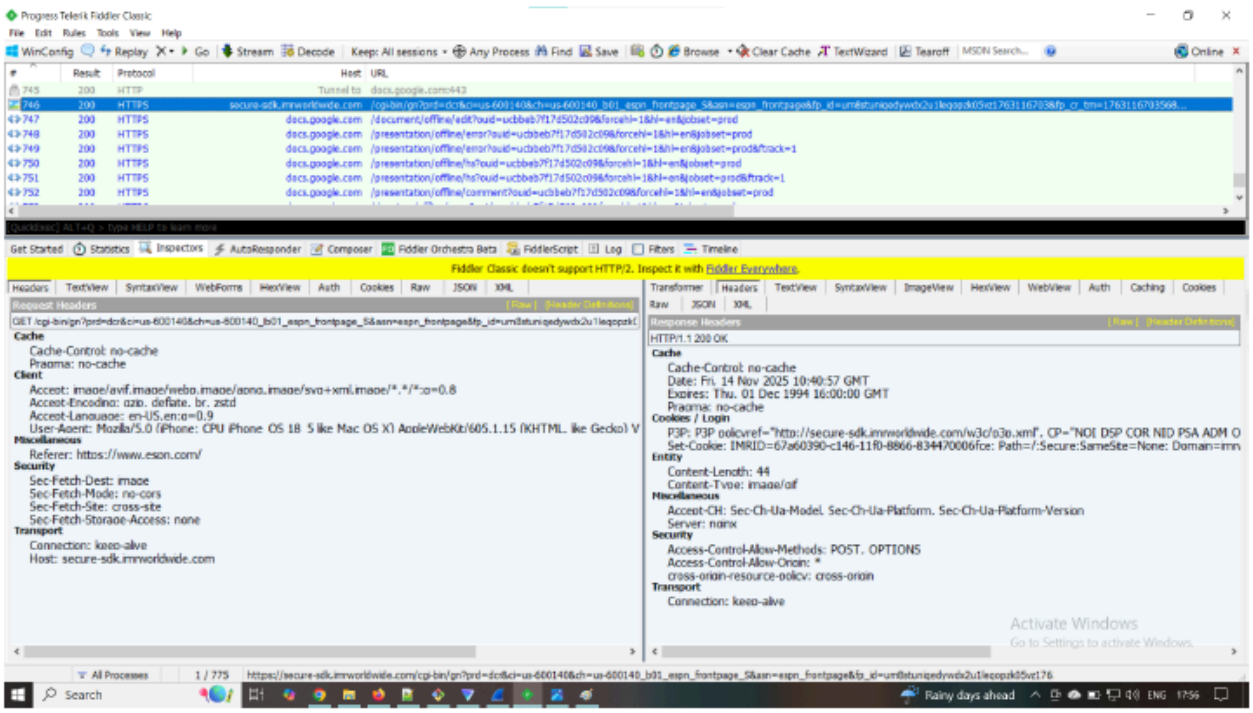
/ / /

/ / /

/ / /

/ / /

Figure 21:



172. The Comscore evidence demonstrates that Defendant designed the Website so that Comscore's tracking infrastructure would activate automatically upon the user's arrival, causing the user's device to transmit her full page-location and referrer information, complete device-fingerprinting attributes, session-level measurement parameters, and her source IP address to Comscore's servers and DNS infrastructure. Figures 17 and 18 show the transmission of detailed behavioral, navigational, and device-identifying metadata; Figures 20 and 21 provide real-time packet-level confirmation of the HTTP requests and responses exchanged with Comscore; and Figure 19 confirms that the user's IP address was communicated during DNS resolution for Comscore's tracking domains. Taken together, these transmissions reveal personal behavioral information about the user's interaction with the Website and identifying information about the device she used, all of which were acquired by Comscore as a direct result of Defendant's embedded tracking scripts operating without the user's knowledge or consent.

/ / /

173. The Comscore tracking code constitutes a "process" because it consists of software and scripts that execute on a user's device to identify the user, gather information about the user and the user's device, and correlate that information across sessions. It also constitutes a "device," because it functions as software installed and executed on computing equipment for the purpose of collecting information. See *James v. Walt Disney Co*., 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

174. Comscore's tracking beacons function as a pen register and/or trap-and-trace device under Cal. Penal Code § 638.50 because they capture outgoing metadata including full page URLs, referrer headers, timestamps, cookies, and browser-level identifiers and receive inbound server-address data and set-cookie information. These exchanges constitute the acquisition of addressing, signaling, routing, and device-identification information prohibited by § 638.51.

175. Defendant did not obtain a court order authorizing the installation or operation of a pen register or trap-and-trace device and did not obtain the user's consent for the activation of Comscore's tracking systems.

176. By embedding and enabling Comscore's scorecardresearch.com and sb.scorecardresearch.com tracking code without the user's consent or judicial authorization, Defendant violated Cal. Penal Code § 638.51

VI. CLASS ALLEGATIONS

177. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class" or "Class Members") defined as follows:

> All persons within California whose browser was subject to installation, execution, embedding, or injection of the Trackers by the Defendant's Website during the relevant statute of limitations period.

178. **NUMEROSITY**: Plaintiff does not know the number of Class Members but believes the number to be in the thousands, if not more. The exact identities of Class Members can be ascertained by the records maintained by Defendant.

/ / /

179. **COMMONALITY**: Common questions of fact and law exist as to all Class Members and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

- Whether Defendant installed, executed, embedded or injected the Trackers on the Website;
- Whether the Trackers are each a pen register and/or trap and trace device as defined by law;
- Whether Plaintiff and Class Members are subject to same tracking policies and practices;
- Whether Plaintiff and Class Members are entitled to statutory damages;
- Whether Class Members are entitled to injunctive relief; and
- Whether the Defendant's conduct violates CIPA.

180. **TYPICALITY**: As a person who visited Defendant's Website and whose outgoing electronic information was surreptitiously collected by the Trackers, Plaintiff is asserting claims that are typical of the Class Members. Plaintiff's experience with the Trackers is typical to Class Members.

181. **ADEQUACY**: Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class or whose inclusion would otherwise be improper are excluded.

182. **SUPERIORITY**: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class Members is impracticable and inefficient. Even if every Class Member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against Defendant

183. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

184. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

185. Defendant uses a pen register device or process and/or a trap and trace device or process on its Website by deploying the Trackers because the Trackers are designed to capture the IP address, User Information and other information such as the phone number, email, routing, addressing and/or other signaling information of website visitors.

186. Defendant did not obtain consent from Plaintiff or any of the Class Members before using pen registers or trap and trace devices to locate or identify users of its Website and has thus violated CIPA. CIPA imposes civil liability and statutory penalties for violations of § 638.51. Cal. Penal Code § 637.2; Moody v. C2 Educational Systems, Inc., No. 2:24-cv-04249-RGK-SK, 2024 U.S. Dist. LEXIS 132614 (C.D. Cal. July 25, 2024).

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following:

1. An order certifying the Class, naming Plaintiff as Class representative, and naming Plaintiff's attorneys as Class counsel;
2. An order declaring that Defendant's conduct violates CIPA;
3. An order of judgment in favor of Plaintiff and the Class against Defendant on the causes of action asserted herein;
4. An order enjoining Defendant's conduct as alleged herein;
5. Statutory damages pursuant to CIPA;
6. Prejudgment interest;

7. Reasonable attorney's fees and costs; and

8. All other relief that would be just and proper as a matter of law or equity.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so permitted.

Dated: December 26, 2025

Respectfully submitted,

NATHAN & ASSOCIATES, APC

By: */s/ Reuben D. Nathan*
Reuben D. Nathan

Reuben D. Nathan, Esq. (SBN 208436)
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff

ClassAction.org
